

**Children's Privacy and Video Games: Comments on Commercial Surveillance ANPR,
R111004¹**

Michael J. S. Beauvais, JD, MSc, Faculty of Law, University of Toronto, Canada

Sara M. Grimes, PhD, Faculty of Information, University of Toronto, Canada

Darshana Jayemanne, PhD, School of Design and Informatics, Abertay University, UK

Seth Giddings, PhD, Winchester School of Art, University of Southampton, UK

The authors are a group of interdisciplinary scholars with expertises in children's media, video games, political economy, privacy, and data protection law.

November 21, 2022

¹ Please send correspondence to Prof. Sara M. Grimes <sara.grimes@utoronto.ca>. The authors are thankful for the assistance of Bronwyn Swerdfager and Alan Bui in preparing these comments.

Comments on Commercial Surveillance ANPR, R111004

Table of Contents

Executive Summary	2
Recommendations	4
Responses to Questions	5
Response to Question b	5
Response to Question 13	8
Response to Question 14	14
Response to Question 17	19
Response to Question 18	21
Response to Question 19	22
Response to Question 21	24
Response to Question 22	25

Executive Summary

We welcome the opportunity to submit the following in response to the Federal Trade Commission’s August 22, 2022 request for comments regarding its Advanced Notice of Proposed Rulemaking (ANPR) on commercial surveillance and data security practices. We are a group of international experts in the areas of children’s digital technologies, ethics, law and policy, specializing in video games and privacy. We are currently collaborating on a multi-year investigation of the reach and impact of commercial surveillance and other under-regulated industry practices in children’s video games and apps.² We are contributing to this call for comments because the US is a global leader in the video game industry, and because US policies are far-reaching and often set the tone for regulation and industry standards of practice in other countries.

We have answered questions b, 13, 14, 17, 18, 19, 21, and 22. We have also included our summarized recommendations at the end of this executive summary. Our full responses give greater context and rationale to the positions for which we advocate here. While the majority of our recommendations and rationales are rooted in evidence pertaining to children’s video games, we believe that they capture more generalizable issues surrounding commercial surveillance and children. Indeed, video games and the data science practices that feature in today’s gaming environment are the product of cross-fertilization between other data-intensive industries.³ Our research and extensive knowledge of

² The Children and Age-Appropriate Game Design project is funded by the Social Sciences and Humanities Research Council of Canada (SSHRC). Dr. Jayemanne’s contributions are funded by the Arts and Humanities Research Council no. AH/S002871/1 (InGAME: Innovation for Games and Media Enterprise).

³ Magy Seif El-Nasr et al., *Game Data Science* (Oxford, New York: Oxford University Press, 2021).

the children’s tech industries, regulatory trends, and children’s own experiences of the digital environment informs our responses to the ANPR.

Video games are an important part of American social and economic life: 75% of US households have at least one gamer and the global video game market is valued at \$159.3 billion as of 2020.⁴ According to the Entertainment Software Association, 71% of kids under the age of 18 in the US regularly play video games.⁵ As described below, playing and connecting with others through video games can be beneficial to children’s learning, socialization, and wellbeing.⁶ However, the widespread use of video games on connected consoles, phones, and tablets raises a number of concerns related to commercial surveillance, primarily related to children’s privacy, commercial exploitation, and dark patterns. Many of these concerns are found across digital applications and services targeted to children (e.g., personal data collection). Some are unique to digital games (e.g., gamblification). We take an expansive definition of “privacy” for the purposes of these comments: privacy denotes the rules that govern flows of personal information. The size and prominence of the video gaming industry in the lives of young people undergirds their heightened responsibility with respect to the privacy and wellbeing of children.

The Commission’s ANPR dovetails with increased interest from policymakers around the globe to understand the changes the digital environment brings to childhood and adolescence and to create rules that ensure that the digital environment supports the varied experiences of young citizens. The UN’s Committee on the Rights of the Child’s *General comment No. 25 on children’s rights in relation to the digital environment* (2021) was written in collaboration with 709 children living in 28 countries and shows that children’s perspectives provide valuable insight into their experiences in the digital environment, their worries and fears surrounding it, and the risks and harms to which they are exposed. The document explicitly calls for governments, policy-makers and regulators to consider children’s needs and implement regulations that render the Internet a safer space for them to use; children do not *want* to be at risk of harm or exposed to disturbing content or users.

Importantly, we are relying heavily upon research findings that derive from children’s input and that center children in the discourse surrounding their online experiences. We believe that the Commission should consider our breadth of experience and expertise in relation to child rights and the digital environment, and draw from the works cited within this submission that showcase children’s lived realities online. We thank you for taking the necessary steps to incorporate children’s views into your work and keenly invite any further correspondence on this matter that would be of service to your office.

⁴ “Media & Entertainment Video Games Sector,” International Trade Administration, accessed November 18, 2022, <https://www.trade.gov/media-entertainment-video-games-sector>.

⁵ “2022 Essential Facts About the Video Game Industry” (Washington, DC: Entertainment Software Association, 2022), <https://www.theesa.com/wp-content/uploads/2022/06/2022-Essential-Facts-About-the-Video-Game-Industry.pdf>.

⁶ See Sara M. Grimes, *Digital Playgrounds: The Hidden Politics of Children’s Online Play Spaces, Virtual Worlds, and Connected Games* (Toronto: University of Toronto Press, 2021), for a critical and comprehensive review of the evidence of these benefits found in multiple studies from across numerous disciplines.

Recommendations

Throughout this submission, we encourage the Commission to:

- Take into consideration the purportedly innocuous nature of play in determining whether a practice is unfair or deceptive.
- Prohibit the collection of data in certain contexts, such as chats and other technologies that facilitate peer-to-peer interactions in games.
- Ensure that rules and guidance are feasible given the market realities for smaller game developers and do not inadvertently favor large game developers.
- Issue guidelines about age-appropriate design elements as a means to prevent deceptive design and associated manipulative design, in ways that are responsive and reflective of children's diverse and ever-changing maturity and literacy, and modes of engagement.
- Develop context-sensitive guidelines for the gaming industry for issues such as loot boxes.
- Continue to develop the notions of unfair and/or deceptive practices in the context of children's goods and services and consider children's views in doing so.
- Take into consideration the purportedly innocuous nature of play in determining whether a practice is unfair or deceptive.
- Better regulate the privacy effects and competition dynamics of third-party application libraries.
- Adopt a proportionate approach to verifiable parental consent and age-assurance systems.
- Furnish children with a robust right to delete their personal information.
- Prioritize flexible and practicable approaches to issues such as the prolonging of online activity.
- Subject user-generated content to more robust privacy rules.
- Complement age-based thresholds with rules that allow for the unique circumstances and capacities of each child to be taken into account.
- Ensure that age-based categories are responsive to the issue at hand and acknowledge their limitations as heuristics.
- Focus less on parental consent and focus more on lifting privacy protections for all users.
- Craft guidance for industry about acceptable information practices should the Commission opt to develop more robust authentication procedures underpinning parental consent.
- For personalized advertising, pursue three options in order of preference: only permit contextual advertising for children's platforms, develop standards for personalized advertising around the notion of the best interests of the child, or develop standards based around the notion of harm.
- Develop a proportional, risk-based approach to its privacy rules; riskier information processing should require more safeguards while less risky ones should be subject to robust, but less onerous safeguards.

Responses to Questions

Response to Question b

To what extent do commercial surveillance practices or lax data security measures harm children, including teenagers?

Children are at a clear disadvantage in their interactions with commercial surveillance practices and at a heightened risk of harm from such practices. This is due in part to children's limited capacity to understand the complexities of contemporary big data processing and thus give meaningful consent to these practices, as well as to their widely varying and developing literacies in conjunction with their marginalized economic and legal status. It is also due to the lack of transparency and openness that many commercial entities have when it comes to user surveillance and how this data is used. Many commercial surveillance practices happen "behind the screen," hidden and poorly communicated to children and their parents. Nonetheless, research shows that children themselves view commercial surveillance practices and lax data security as harmful, and identify these issues among their topmost concerns when it comes to the digital environment. Children and adolescents also worry about how data collected about them by commercial entities might negatively impact future life opportunities.⁷

Research conducted since the late 1990s has traced the continued proliferation and expansion of corporate surveillance and data collection practices throughout the children's digital landscape.⁸ From websites and videogames, to virtual assistants and the "Internet of Toys," businesses have steadily used connected technologies to gather vast amounts of personal and behavioral information from children. The full implications of ubiquitous "dataveillance" and the various ways that children's data is ultimately used (and abused) over the course of their lifetimes are not yet known. But it is clear that fundamental, and historically private, experiences of childhood are transformed as commercial entities and priorities insert themselves into children's play, identity-formation, and interactions with friends and family.

Children's information is used to track them, advertise to them, and encourage them to engage in practices that generate revenue for corporations (operators, advertisers, data brokers, etc.). In the case

⁷ Amanda Third et al., *Young People in Digital Society: Control Shift*, Studies in Childhood and Youth (London: Palgrave Macmillan, 2019).

⁸ Kathryn C. Montgomery, *Generation Digital: Politics, Commerce, and Childhood in the Age of the Internet* (Cambridge, MA: The MIT Press, 2007), <https://doi.org/10.7551/mitpress/3222.001.0001>; Veronica Barassi, *Child | Data | Citizen: How Tech Companies Are Profiling Us from before Birth* (Cambridge, MA: The MIT Press, 2020); Donell Holloway, "Surveillance Capitalism and Children's Data: The Internet of Toys and Things for Children," *Media International Australia* 170, no. 1 (February 1, 2019): 27–36, <https://doi.org/10.1177/1329878X19828205>; Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019); Jennifer Ann Hill, "Endangered Childhoods: How Consumerism Is Impacting Child and Youth Identity," *Media, Culture & Society* 33, no. 3 (April 1, 2011): 347–62, <https://doi.org/10.1177/0163443710393387>; Sara M Grimes, "Playing by the Market Rules: Promotional Priorities and Commercialization in Children's Virtual Worlds," *Journal of Consumer Culture* 15, no. 1 (March 1, 2015): 110–34, <https://doi.org/10.1177/1469540513493209>.

of in-game loot boxes and other forms of “gamblification,” detailed below, children’s information is used to optimize the likelihood of real money purchases and minimize player disengagement (e.g., timing a “lucky” reward to appear when players are most likely to turn the game off in order to encourage them to keep playing). These practices are designed to anticipate and guide children towards activities and content that are disruptive and potentially harmful. For instance, prolonging gameplay necessarily detracts time and attention from other activities a child might engage in (leisure, homework, etc.), and can disrupt children’s ability to follow household limits on “screen time” thereby causing conflict between children and parents and/or caregivers.⁹

Children’s subordinate role within most economic transactions is a key factor for considering the nature and extent of the harms afforded by commercial surveillance. Very few children have the authority or ability to make in-game or in-app purchases on their own, and require parental involvement and consent. This was previously acknowledged by the Commission in 2014 when it required Apple to refund parents for in-app purchases made by their children without parental consent and to change its billing practices to ensure express parental consent for each purchase moving forward.¹⁰ Moreover, children and teens have varying and still developing levels of economic socialization and literacy, with gaps in knowledge that can currently be exploited for commercial gain (e.g., through marketing practices that make it difficult or impossible for children to distinguish ads from the game itself). Many children’s games also contain real money transactions that are necessary in order to win, progress, or even access key aspects of the gameplay. Commercial surveillance is thus used to perpetuate “hierarchies of access” wherein some children are allowed more and deeper kinds of participation and privileges than others, based on factors beyond their control.¹¹ These practices evoke and exploit feelings of longing (for access, for fun, for virtual items) and belonging (to peer groups and game communities) with negative consequences for children’s emotional well-being.¹²

Notably, most children and teens are themselves concerned about commercial surveillance practices and lax data security, and the associated harms to their current and future wellbeing. In a far-ranging consultation with over 700 children (aged 8 to 18 years) in 27 countries conducted under the auspices of the United Nations’ Committee on the Rights of the Child in preparation for its *General comment No. 25 (2021) on children’s rights in relation to the digital environment*, most children reported that

⁹ Sarah E. Domoff et al., “Prevalence and Predictors of Children’s Persistent Screen Time Requests: A National Sample of Parents,” *Human Behavior and Emerging Technologies* 3, no. 5 (December 2021): 700–709, <https://doi.org/10.1002/hbe2.322>.

¹⁰ “Apple Inc. Will Provide Full Consumer Refunds of At Least \$32.5 Million to Settle FTC Complaint It Charged for Kids’ In-App Purchases Without Parental Consent,” Federal Trade Commission, January 15, 2014, <https://www.ftc.gov/news-events/news/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million-settle-ftc-complaint-it-charged-kids>.

¹¹ Sara M. Grimes and Deborah A. Fields, “Kids Online: A New Research Agenda for Understanding Social Networking Forums” (New York: Joan Ganz Cooney Center at Sesame Workshop, 2012), https://joanganzcooneycenter.org/wp-content/uploads/2012/11/jgcc_kidsonline.pdf.

¹² Allison Pugh, *Longing and Belonging: Parents, Children, and Consumer Culture* (Berkeley and Los Angeles, California: University of California Press, 2009).

they wanted greater transparency from companies about information processing.¹³ Only 36% of them felt that sharing interests and preferences with companies was okay, and less than a third said they would share personal information with companies if they had a choice. Across these countries, children expressed unease with how their data, including their likes, dislikes and online activities, is surveilled and used by commercial entities. Many of them “worried that others—known and unknown to them—might use this data in ways that can negatively impact their security, safety and wellbeing”.¹⁴ Furthermore, half of participants expressed that they had had scant opportunities to learn about protecting their data online. These findings are useful for understanding the interrelated issues of agency, digital literacy, and socioeconomic position with respect to children’s position as citizens and consumers of goods and services that process their data. While most of the children who participated in the study emphasized the many potential benefits of the digital environment, the majority called for “stronger legislation and/or regulation to address how companies access and use their personal data”.¹⁵

An important way that commercial surveillance practices and lax data protection harm children is through the infringement of children’s rights, including the right to privacy, the right to play, the right not to be exploited, and the right to be heard. The extent of these harms varies across platforms and age groups, but evidence of their prevalence is well documented.¹⁶ The United States is the only UN Member State to have signed but not ratified the *Convention on the Rights of the Child* (CRC). The objections to ratification are likely overstated.¹⁷ Even though the United States has not ratified the CRC, it can still build upon internationally recognized best practices that use a children’s rights framework when it comes to policymaking on matters affecting children. The *Family Educational Rights and Privacy Act* and COPPA, for example, are among the principal ways in which American children’s rights to privacy are secured. We further note that one of the CRC’s main principles - the best interests of the child - is commonly used in US family law.¹⁸ States’ laws also incorporate aspects of the CRC. For example, the *California Age-Appropriate Design Code Act* also expressly mentions the CRC.¹⁹

¹³ Amanda Third and Lilly Moody, “Our Rights in the Digital World: A Report on the Children’s Consultations to Inform UNCRC General Comment 25” (London and Sydney: 5Rights Foundation and Western Sydney University, 2021), <https://5rightsfoundation.com/uploads/OurRightsinaDigitalWorld-FullReport.pdf>.

¹⁴ Third and Moody, 42.

¹⁵ Third and Moody, 51.

¹⁶ Sonia Livingstone, Gerison Lansdown, and Amanda Third, “The Case for a UNCRC General Comment on Children’s Rights and Digital Media” (London: Children’s Commissioner for England and LSE Consulting, 2017), <https://www.lse.ac.uk/business/consulting/assets/documents/the-case-for-a-uncrc-general-comment-on-childrens-rights-and-digital-media.pdf>; Grimes, *Digital Playgrounds*.

¹⁷ Lainie Rutkow and Joshua T. Lozman, “Suffer the Children: A Call for United States Ratification of the United Nations Convention on the Rights of the Child,” *Harvard Human Rights Journal* 19 (2006): 161–90.

¹⁸ Lynne Marie Kohm, “Tracing the Foundations of the Best Interests of the Child Standard in American Jurisprudence,” *Journal of Law & Family Studies* 10, no. 2 (2008 2007): 337–76.

¹⁹ “The California Age-Appropriate Design Code Act.,” AB-2273 § (2022), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273.

Response to Question 13

The Commission here invites comment on commercial surveillance practices or lax data security measures that affect children, including teenagers. Are there practices or measures to which children or teenagers are particularly vulnerable or susceptible? For instance, are children and teenagers more likely than adults to be manipulated by practices designed to encourage the sharing of personal information?

Yes, children and teenagers can be particularly vulnerable to surveillance practices. However, much depends on the child and the context in which data are collected. We encourage the Commission to prohibit the collection of data in certain contexts, such as chats and other technologies that facilitate peer-to-peer interactions in games. We furthermore encourage the Commission to issue guidelines about age-appropriate design elements as a means to prevent deceptive design and associated manipulative design, in ways that are responsive and reflective of children's diverse and ever-changing maturity and literacy, and modes of engagement. In support of this response, this section provides an evidence-based rationale about the evolving capacities of children and teenagers to understand and consent to commercial surveillance and advertising practices, as well as assess data security risks. We then describe some of the practices to which children and teenagers are particularly vulnerable, including manipulative design (behavioral advertising and profiling), loot boxes and other in-game purchase-based systems that reproduce (or closely mimic) those used by the gambling industry (often referred to as the "gamblification" of video games).

Children's and teens' capacities to understand surveillance practices and advertising

Children and teens have varying levels of literacy and awareness of commercial surveillance practices and data security. While some young people are well informed and able to make good decisions about how they engage and how they share their data online, many others do not have access to the resources and support (educational, parental/familial, etc.) required for robust consent. Teens are particularly underserved by the US data protection landscape because COPPA's protections do not cover them, yet they display difficulties in understanding issues material to protecting their privacy.

In a systemic evidence mapping of children's understanding of personal data and privacy online, Stoilova and colleagues noted that studies tended to show that children younger than eight look to adults for what to do with respect to information disclosure.²⁰ Between eight and 11 years of age, children begin to identify issues regarding how sharing information may create risks. From the age of 12 onwards, children are more discerning regarding information disclosure. Despite this, an ongoing issue is that even 17-year-olds display a poor understanding of data collection practices, with one study

²⁰ Mariya Stoilova, Rishita Nandagiri, and Sonia Livingstone, "Children's Understanding of Personal Data and Privacy Online – a Systematic Evidence Mapping," *Information, Communication & Society*, September 17, 2019, 1–19, <https://doi.org/10.1080/1369118X.2019.1657164>; Mariya Stoilova, Sonia Livingstone, and Rishita Nandagiri, "Digital by Default: Children's Capacity to Understand and Manage Online Data and Privacy," *Media and Communication* 8, no. 4 (November 10, 2020): 197–207.

evidencing that young people’s understanding of data collection practices does not reach a “mature level” until the age of 20.²¹

In particular, children demonstrate difficulty in understanding two aspects that are material to their ability to navigate commercial surveillance and data security. First, they fail to understand the relationships between pieces of information and instead think about pieces of information in isolation. This is particularly concerning in the face of complex processes of data aggregation done by data brokers.²² Children may disclose discrete pieces of information believing them to be less revealing than what they actually are. They may moreover be more focused on active disclosure and not take account of the data exhaust or traces left by their online activities.²³ Second, children may fail to understand the commercial relationship they have with online services and the economic model that underpins the processing of their data. Instead of seeing a platform as a commercial entity with its own agenda and business model, children have been found to transpose the trust they place in interpersonal data sharing onto the commercial relationship.²⁴ When engaging in in-game chat with other players, creating user-generated content, or participating in other expressive activities, then, children may be more focused on the question of whether they should disclose something to their audience instead of also considering the surveillance practices of the infrastructure that facilitates their interactions.²⁵

These findings concerning surveillance dovetail with those regarding children’s understanding of advertising. Results from a recent study suggest that children’s advertising literacy reaches a “mature level” at 16 years of age but that their data collection literacy does not do so until 20 years of age.²⁶ Furthermore, the OECD has found that “[c]hildren have insufficient understanding of how Internet

²¹ Brahim Zarouali et al., “Adolescents’ Advertising Literacy and Privacy Protection Strategies in the Context of Targeted Advertising on Social Networking Sites: Implications for Regulation,” *Young Consumers* 21, no. 3 (January 1, 2020): 351–67, <https://doi.org/10.1108/YC-04-2020-1122>.

²² Adam J. Andreotta, Nin Kirkham, and Marco Rizzi, “AI, Big Data, and the Future of Consent,” *AI & SOCIETY*, August 30, 2021, <https://doi.org/10.1007/s00146-021-01262-5>; Fred H. Cate and Viktor Mayer-Schönberger, “Notice and Consent in a World of Big Data,” *International Data Privacy Law* 3, no. 2 (May 1, 2013): 67–73, <https://doi.org/10.1093/idpl/ipr005>.

²³ Sara M. Grimes, “Child-Generated Content: Children’s Authorship and Interpretive Practices in Digital Gaming Cultures,” in *Dynamic Fair Dealing: Creating Canadian Culture Online*, ed. Rosemary Coombe, Darren Wershler, and Martin Zeilinger (Toronto: University of Toronto Press, 2014), 336–46, <https://doi.org/10.3138/9781442665613>; Laurien Desimpelaere, Liselot Hudders, and Dienneke Van de Sompel, “Children’s Perceptions of Fairness in a Data Disclosure Context: The Effect of a Reward on the Relationship between Privacy Literacy and Disclosure Behavior,” *Telematics and Informatics* 61 (August 1, 2021): 101602, <https://doi.org/10.1016/j.tele.2021.101602>; Stoilova, Livingstone, and Nandagiri, “Digital by Default.”

²⁴ Valerie Steeves, “Privacy, Sociality and the Failure of Regulation: Lessons Learned from Young Canadians’ Online Experiences,” in *Social Dimensions of Privacy: Interdisciplinary Perspectives*, ed. Beate Roessler and Dorota Mokrosinska (Cambridge, UK: Cambridge University Press, 2015), 244–60, <https://doi.org/10.1017/CBO9781107280557>; Valerie Steeves and Priscilla Regan, “Young People Online and the Social Value of Privacy,” *Journal of Information, Communication and Ethics in Society* 12, no. 4 (January 1, 2014): 298–313, <https://doi.org/10.1108/JICES-01-2014-0004>.

²⁵ Zarouali et al., “Adolescents’ Advertising Literacy and Privacy Protection Strategies in the Context of Targeted Advertising on Social Networking Sites.”

²⁶ Zarouali et al.

content is produced and financed, which is also a reason why they have difficulty critically assessing advertising messages.”²⁷ In the above mentioned international children’s consultation conducted for the *General Comment No. 25*, researchers found that while most children identified branding (82%) and advertising (67%) as key influences on their consumption habits, their descriptions of these influences were deeply ambiguous, “signaling some of the challenges for building children’s critical digital literacies”.²⁸ For “advergames”, games whose main function is to promote commercial products²⁹, the effect of children’s relative inability to understand surveillance and distinguish commercial messages is glaring: children are encouraged to interact in environments that are designed to push commercial messages and collect data in a variety of ways. Games may also use “rewarded inventory” for engaging with content from other publishers: a player can earn in-game rewards for reading articles or sitting through other commercial content.³⁰ Even in games that rely largely on user-made creations, such as Minecraft and Roblox, advertising seeps into play through sponsored worlds and branded content, turning players’ creations into immersive advertising for third-parties.³¹ This commercialization of play can have negative effects on children’s self-image and how they understand the world around them.³²

Manipulative design and the undermining of self-directed play

A combination of manipulative game design and targeted, behavioral advertising undermines free or self-directed play. For children, free play is essential to their development of social skills and burgeoning autonomy.³³ Free play is increasingly rare in children’s lives due to a combination of overscheduling³⁴, a lack of time for play at school due to increased emphasis on testing³⁵, and underinvestment in

²⁷ OECD, “The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them” (Paris: OECD, May 2, 2011), 25, <https://doi.org/10.1787/5kgcjf71pl28-en>.

²⁸ Third and Moody, “Our Rights in the Digital World: A Report on the Children’s Consultations to Inform UNCRC General Comment 25,” 102.

²⁹ Valerie Verdoodt, Damian Clifford, and Eva Lievens, “Toying with Children’s Emotions, the New Game in Town? The Legality of Advergames in the EU,” *Computer Law & Security Review* 32, no. 4 (August 1, 2016): 599–614, <https://doi.org/10.1016/j.clsr.2016.05.007>.

³⁰ Ryan Barwick and Jenn Brice, “Major Publishers Are Buying Ads in Mobile Games like ‘Subway Surfers’ to Juice Traffic,” *Marketing Brew*, August 11, 2022, <https://www.marketingbrew.com/stories/2022/08/11/major-publishers-are-buying-ads-in-mobile-games-like-subway-surfers-to-juice-traffic>.

³¹ Grimes, *Digital Playgrounds*.

³² Simone van der Hof et al., “‘Don’t Gamble With Children’s Rights’—How Behavioral Design Impacts the Right of Children to a Playful and Healthy Game Environment,” *Frontiers in Digital Health* 4 (May 2, 2022): 822933, <https://doi.org/10.3389/fdgth.2022.822933>.

³³ Pam Jarvis, Stephen Newman, and Louise Swiniarski, “On ‘Becoming Social’: The Importance of Collaborative Free Play in Childhood,” *International Journal of Play* 3, no. 1 (January 2, 2014): 53–68, <https://doi.org/10.1080/21594937.2013.863440>.

³⁴ Alvin Rosenfeld and Nicole Wise, *The Over-Scheduled Child: Avoiding the Hyper-Parenting Trap* (St. Martin’s Publishing Group, 2010).

³⁵ Jarvis, Newman, and Swiniarski, “On ‘Becoming Social.’”

playgrounds and other types of public infrastructures, which disproportionately affects poorer, urban communities³⁶. This makes preserving free play in the digital environment all the more important.

Due to its developmental and social benefits, the undermining of free play harms children in a way that is unlike with adults. The ability to make –negotiate and implement–decisions through peer play contributes significantly to children’s sense of belonging, identity, and group cohesion.³⁷ However, full participation requires a certain amount of agency, autonomy, and ownership—the very things that are subverted by commercial surveillance mechanisms aimed at exploiting, manipulating, and channeling children’s data and online interactions for commercial gain and corporate interests.

Video games, like other forms of dynamic media and platforms, rely on their adaptability to structure our choices based on the various pieces of information they collect and analyze.³⁸ Children, especially younger ones, seem particularly susceptible to such manipulation³⁹ and disproportionately targeted by it⁴⁰. Manipulative design in children’s interactive media, including purchasing pressure and pressure to spend more time playing, has been found to be present in 80% of sampled children’s applications and was more prevalent for children (aged 3 to 5) from households with lower socioeconomic status.⁴¹ These features can undermine intrinsic motivation and free choice in play.⁴²

Understanding whether or not a game’s design is problematic (e.g., uses deceptive design or “dark patterns”) or causes harm is highly contextual, which speaks to the need for principled and flexible regulation. Certain design features may be desirable in one context, but harmful in another.⁴³ For

³⁶ Nina Lakhani, “Millions of Americans Lack Access to Quality Parks, Report Reveals,” *The Guardian*, May 20, 2020, sec. Environment, <https://www.theguardian.com/environment/2020/may/20/park-inequality-access-coronavirus-wellbeing>.

³⁷ William A. Corsaro, “Collective Action and Agency in Young Children’s Peer Cultures,” in *Studies in Modern Childhood: Society, Agency, Culture*, ed. Jens Qvortrup (London: Palgrave Macmillan UK, 2005), 231–47, https://doi.org/10.1057/9780230504929_14.

³⁸ Grimes, “Playing by the Market Rules”; Karen Yeung, “Hypernudge?: Big Data as a Mode of Regulation by Design,” *Information, Communication & Society* 20, no. 1 (January 2, 2017): 118–36, <https://doi.org/10.1080/1369118X.2016.1186713>; Tal Z. Zarsky, “Privacy and Manipulation in the Digital Age,” *Theoretical Inquiries in Law* 20, no. 1 (March 16, 2019): 157–88, <https://doi.org/10.1515/til-2019-0006>; M. Ryan Calo, “Digital Market Manipulation,” *The George Washington Law Review* 82, no. 4 (2014): 995–1051.

³⁹ Gwenn Schurgin O’Keeffe, Kathleen Clarke-Pearson, and Council on Communications and Media, “The Impact of Social Media on Children, Adolescents, and Families,” *Pediatrics* 127, no. 4 (April 1, 2011): 800–804, <https://doi.org/10.1542/peds.2011-0054>.

⁴⁰ Grimes, *Digital Playgrounds*.

⁴¹ Jenny Radesky et al., “Prevalence and Characteristics of Manipulative Design in Mobile Applications Used by Children,” *JAMA Network Open* 5, no. 6 (June 17, 2022): e2217641, <https://doi.org/10.1001/jamanetworkopen.2022.17641>.

⁴² Sonia Livingstone and Kruakae Pothong, “Imaginative Play in Digital Environments: Designing Social and Creative Opportunities for Identity Formation,” *Information, Communication and Society* 25, no. 4 (April 1, 2022): 485–501.

⁴³ José P. Zagal, Staffan Björk, and Chris Lewis, “Dark Patterns in the Design of Games,” in *Proceedings of the 8th International Conference on the Foundations of Digital Games* (Chania, Crete, Greece, 2013), <http://urn.kb.se/resolve?urn=urn:nbn:se:ri:diva-24252>; Leon Y. Xiao and Laura L. Henderson, “Towards an Ethical Game Design Solution to Loot Boxes: A Commentary on King and Delfabbro,” *International Journal of Mental Health and Addiction* 19, no. 1 (February 1, 2021): 177–92, <https://doi.org/10.1007/s11469-019-00164-4>.

example, screen time is considered a poor heuristic for determining whether or not device use is problematic. Research has emphasized that “the content, context, and connections associated with children’s digital engagement” matters more than screen time.⁴⁴ A recent study on adults’ well-being found “little to no evidence for a causal connection between game play and well-being”, but that the motivation behind game play mattered.⁴⁵

When considering making rules for game and related industries, the Commission should consider articulating factors to be weighed on a case-by-case basis. This would allow an approach that is principled and flexible. While clarity and foreseeability are invariably virtues of good regulation, the difficulty in articulating bright-line rules arguably allows deceptive designs to proliferate. Given the importance of play and of the importance of games (including video games) in children’s development, guidelines would enable children to benefit from video games without being subjected to the various privacy harms that deceptive designs may pose. Indeed, during the COVID-19 pandemic research confirmed the positive impact video games can have on children’s and teenagers’ well-being.⁴⁶

Loot boxes and in-game purchases

The combination of personalized nudges based on highly detailed data with monetization strategies based on in-game purchases risks the economic exploitation of children. Consider the case of loot boxes, which “generally provide players with a random chance to receive virtual rewards after meeting certain requirements. Requirements may be a certain amount of time playing the game (time-gating), direct (‘in-app’) purchase with real or in-game currency, or skillful play. The rewards take various forms, but commonly may be: ‘skins’ (looks for a character), lowered ‘cooldowns’ (timers influencing progression in the game), artwork, fantasy or celebrity characters, or in-game currencies. Loot boxes may actually resemble gift-wrapped ‘boxes’, but they may take other audio-visual forms (luminous crystals, eggs which hatch, virtual piñatas, clocks or countdowns) according to the game’s theme.”⁴⁷

⁴⁴ Sonia Livingstone and Kruakae Pothong, “Beyond Screen Time: Rethinking Children’s Play in a Digital World,” *Journal of Health Visiting* 10, no. 1 (January 2, 2022): 32–38.

⁴⁵ Matthew Barr and Alicia Copeland-Stewart, “Playing Video Games During the COVID-19 Pandemic and Effects on Players’ Well-Being,” *Games and Culture* 17, no. 1 (January 1, 2022): 122–39, <https://doi.org/10.1177/15554120211017036>; Pierpaolo Limone and Giusi Antonia Toto, “Psychological and Emotional Effects of Digital Technology on Children in COVID-19 Pandemic,” *Brain Sciences* 11, no. 9 (September 2021): 1126, <https://doi.org/10.3390/brainsci11091126>.

⁴⁶ Barr and Copeland-Stewart, “Playing Video Games During the COVID-19 Pandemic and Effects on Players’ Well-Being”; Limone and Toto, “Psychological and Emotional Effects of Digital Technology on Children in COVID-19 Pandemic.”

⁴⁷ Darshana Jayemanne et al., “Loot Boxes and Digital Gaming: A Rapid Evidence Assessment” (United Kingdom: Department for Digital, Culture, Media & Sport, 2021), 10, https://www.research.ed.ac.uk/files/293610540/Loot_Box_REA.pdf.

Depending on design and context in conjunction with regulatory framework, loot boxes either be considered gambling or very similar to gambling.⁴⁸ Putting legal definitions aside, more concerning is the effect that these features have on users. Multiple studies, using multiple techniques and measures, have demonstrated that problem gambling is linked to loot box usage.⁴⁹ Research has linked loot boxes in video games with the development of problem gambling in older adolescents (16- to 18-year-olds).⁵⁰ This builds on decades of empirical evidence that adolescents are more susceptible to developing emotional, social, or psychological issues in response to online gambling.⁵¹

The number of studies using participants younger than 18 years of age remains small and thus the evidence base is relatively limited.⁵² However, a recent scoping review on the link of loot boxes to problematic gambling among adult players indicates that all studies found a positive association between loot boxes and problematic gambling.⁵³ As the Commission itself has previously emphasized, “Every state prohibits gambling by minors.”⁵⁴ We also note that loot boxes (and other in-game purchases) price things in virtual currencies such that the player cannot easily determine the true cost of acquiring the loot box in dollars and cents.⁵⁵ There is thus a compelling case for taking a *cautious approach* when it comes to including loot boxes in games played by children and adolescents. Designers should be required to prioritize the best interests of the child when deciding if, why, and how to include loot boxes in games.

While the biggest, most highly value-added games (“AAA” or “Triple-A” games)⁵⁶ seem to be shifting away from the use of loot boxes, the trend remains prevalent in the mobile gaming industry. Loot boxes

⁴⁸ Leon Y. Xiao et al., “Regulating Gambling-Like Video Game Loot Boxes: A Public Health Framework Comparing Industry Self-Regulation, Existing National Legal Approaches, and Other Potential Approaches,” *Current Addiction Reports* 9, no. 3 (September 1, 2022): 163–78, <https://doi.org/10.1007/s40429-022-00424-9>.

⁴⁹ Jayemanne et al., “Loot Boxes and Digital Gaming: A Rapid Evidence Assessment.”

⁵⁰ David Zendle, Rachel Meyer, and Harriet Over, “Adolescents and Loot Boxes: Links with Problem Gambling and Motivations for Purchase,” *Royal Society Open Science* 6, no. 6 (June 19, 2019): 190049, <https://doi.org/10.1098/rsos.190049>.

⁵¹ Filipa Calado, Joana Alexandre, and Mark D. Griffiths, “Prevalence of Adolescent Problem Gambling: A Systematic Review of Recent Research,” *Journal of Gambling Studies* 33, no. 2 (June 2017): 397–424, <https://doi.org/10.1007/s10899-016-9627-5>; Marc N. Potenza et al., “Correlates of At-Risk/Problem Internet Gambling in Adolescents,” *Journal of the American Academy of Child and Adolescent Psychiatry* 50, no. 2 (February 2011): 150–159.e3, <https://doi.org/10.1016/j.jaac.2010.11.006>; R. Andrew Chambers and Marc N. Potenza, “Neurodevelopment, Impulsivity, and Adolescent Gambling,” *Journal of Gambling Studies* 19, no. 1 (2003): 53–84, <https://doi.org/10.1023/a:1021275130071>.

⁵² Irene Montiel et al., “Loot Box Engagement: A Scoping Review of Primary Studies on Prevalence and Association with Problematic Gaming and Gambling,” ed. Marc Potenza, *PLOS ONE* 17, no. 1 (January 27, 2022): e0263177, <https://doi.org/10.1371/journal.pone.0263177>.

⁵³ Montiel et al.

⁵⁴ “FTC Warns Consumers about Online Gambling and Children | Federal Trade Commission,” June 26, 2002, <https://www.ftc.gov/news-events/news/press-releases/2002/06/ftc-warns-consumers-about-online-gambling-children>.

⁵⁵ Xiao and Henderson, “Towards an Ethical Game Design Solution to Loot Boxes.”

⁵⁶ D. B. Nieborg, “Triple-A: The Political Economy of the Blockbuster Video Game” (doctoral thesis, Amsterdam, University of Amsterdam, 2011), <https://hdl.handle.net/11245/1.345555>.

are still present in games that may well be played by young people such as EA Sports' FIFA series.⁵⁷ Furthermore, the case of loot boxes may be precursor to other problematic approaches to monetization in the games industry. Similar techniques such as "battle passes" from Valve Corporation's *DOTA 2*, Activision Blizzard in *Diablo Immortal* and *Overwatch 2* have been critiqued for their exploitative designs with opaque pricing, undermining of player equality, and their availability only after players have invested time in the game.⁵⁸ Meanwhile, a recent study found that 42% of the top-grossing mobile games rated as suitable for players aged 4 years and over on the iPhone, and 40% of those rated as suitable for players aged 3 years and over on Android, contained loot boxes.⁵⁹

We think it is important for the Commission to continue to develop its approach in interpreting the notions of unfair and/or deceptive practices in the context of children's goods and services. For the digital environment in particular, children are situated in a choice architecture that they themselves will have had little or even no say in its design. Children's greatly reduced economic power moreover means that they cannot navigate the market in the same manner as adults, i.e., many practices are "not reasonably avoidable by consumers themselves"⁶⁰ and many children don't fully understand the commercial relationships and processes at work within immersive commercial practices.

Response to Question 14

What types of commercial surveillance practices involving children and teens' data are most concerning? For instance, given the reputational harms that teenagers may be characteristically less capable of anticipating than adults, to what extent should new trade regulation rules provide teenagers with an erasure mechanism in a similar way that COPPA provides for children under 13? Which measures beyond those required under COPPA would best protect children, including teenagers, from harmful commercial surveillance practices?

We propose the Commission consider four aspects of commercial surveillance practices in video games. First, how the purportedly innocuous nature of play may be used to shroud business models and deceptive practices. Second, how the widespread use of third-party application libraries in games can undermine children's privacy in unexpected ways. Third, how the need for verifiable parental consent and associated age-assurance systems without sufficient guardrails can undermine the privacy of children and their parents. Fourth, how furnishing children with a generous right to erasure of their

⁵⁷ Joshua Robertson, "EA To Continue Using Loot Boxes In FIFA 23," *TheGamer*, August 11, 2022, <https://www.thegamer.com/fifa-23-loot-boxes-ea/>.

⁵⁸ Andrei Zanesco, Martin French, and Marc Lajeunesse, "Betting on DOTA 2's Battle Pass: Gambification and Productivity in Play," *New Media & Society* 23, no. 10 (October 1, 2021): 2882–2901, <https://doi.org/10.1177/1461444820941381>; Daniel Joseph, "Battle Pass Capitalism," *Journal of Consumer Culture* 21, no. 1 (February 1, 2021): 68–83, <https://doi.org/10.1177/1469540521993930>.

⁵⁹ David Zendle et al., "The Prevalence of Loot Boxes in Mobile and Desktop Games," *Addiction* 115, no. 9 (September 2020): 1768–72, <https://doi.org/10.1111/add.14973>.

⁶⁰ 15 USC § 45(n)

data held by companies, which includes notification obligations on the part of companies, can help young people in the transition to adulthood.

Games and the purportedly innocuous nature of play

We recommend that the Commission take into consideration the purportedly innocuous nature of play in determining whether a practice is unfair or deceptive. Data protection rules like COPPA furthermore do not *per se* ensure that the digital environment, including games, align with children's best interests or consider the totality of their rights.

An overarching concern specific to the gaming industry is how games are viewed as seemingly innocuous spaces where users can play and let their guard down. Indeed, games are meant to provide spaces where users can focus on the games' objectives. This picture shrouds the real-world implications of the pervasive commercial surveillance that often occurs in children's digital play spaces. This repositions "play" as a form of market exchange and forum for commercial surveillance and can undermine "play" as a site for children to develop skills and exercise imagination, and engage in community-building and meaning-making with peers.⁶¹

Commercial surveillance and behavioral targeting may also exploit nascent identity formation in funneling children into particular groups that hinders their ability to experiment with identities and beliefs.⁶² This is all the more concerning when one considers that children commonly see games and other sites of play as "their" spaces, built for their enjoyment and with their interests as the priority.⁶³ Playful applications may furthermore be used to obfuscate and normalize controversial technologies/practices such as the use of biometrics.⁶⁴ With increased attention (and resources) going to the development of virtual reality (VR) devices and platforms, these privacy issues are likely to intensify. See, for example, the highly invasive physiological data collection practices of Meta's newest VR headset.⁶⁵

Third-party application libraries

⁶¹ Pugh, *Longing and Belonging*; Grimes, *Digital Playgrounds*.

⁶² Eva Lievens, "Growing Up with Digital Technologies: How the Precautionary Principle Might Contribute to Addressing Potential Serious Harm to Children's Rights," *Nordic Journal of Human Rights* 39, no. 2 (April 3, 2021): 128–45, <https://doi.org/10.1080/18918131.2021.1992951>.

⁶³ Sara M. Grimes and Vinca Merriman, "Technically They're Your Creations, but ...': Children Making, Playing, and Negotiating User-Generated Content Games," in *The Routledge Companion to Digital Media and Children*, ed. Lelia Green et al. (Routledge, 2020), 275–84, <https://doi.org/10.4324/9781351004107-26>; Rebekah Willett, "Consumer Literacies and Virtual World Games," in *The Routledge Handbook of Literacy Studies* (Routledge, 2015); Rebekah Willett, "Microsoft Bought Minecraft ... Who Knows What's Going to Happen?!: A Sociocultural Analysis of 8–9-Year-Olds' Understanding of Commercial Online Gaming Industries," *Learning, Media and Technology* 43, no. 1 (2016): 101–16, <https://doi.org/10.1080/17439884.2016.1194296>.

⁶⁴ Ariane Ellerbrok, "PLAYFUL BIOMETRICS: Controversial Technology through the Lens of Play," *The Sociological Quarterly* 52, no. 4 (2011): 528–47.

⁶⁵ Khari Johnson, "Meta's New Quest Pro VR Headset Harvests Personal Data Right Off Your Face," *WIRED*, October 13, 2022, <https://www.wired.com/story/metax-vr-headset-quest-pro-personal-data-face/>.

One of the most problematic issues facing children’s privacy in video games concerns the use of third-party libraries included in application programming interfaces (APIs) and in software development kits (SDKs). Here, children’s privacy comes into contact with uncompetitive markets and opaque information processing pipelines. Developers will use these third-party libraries to serve ads on their users, which are provided by large intermediary advertising networks.⁶⁶ Serving targeted ads relies upon user data and so these third-party libraries suck up data about users and facilitate the creation of user profiles.⁶⁷ Users are typically unaware of such data collection and even developers themselves face difficulties navigating their options.⁶⁸ The July 2022 merger agreement between Unity and ironSource demonstrates the strong commercial links between game development and monetization strategy.⁶⁹ Even if such mergers are not problematic from the perspective of antitrust law, they are from the perspective of privacy. There is evidence that these techniques are efficacious in influencing children⁷⁰, although there are gaps in our knowledge of how age differences affect literacy around ads served within a game context.

Advertising is a particularly important revenue stream for “free to play” (F2P) games.⁷¹ Given that use of the application (pending no ‘freemium’ option that removes ads) requires the serving of ads, users typically do not have a choice with respect to how their data are used. F2P games are popular among children.⁷² F2P games are an important stream of children’s data for advertising networks, which are

⁶⁶ Dan Fitton and Janet C. Read, “Creating a Framework to Support the Critical Consideration of Dark Design Aspects in Free-to-Play Apps,” in *Proceedings of the 18th ACM International Conference on Interaction Design and Children*, IDC ’19 (New York, NY, USA: Association for Computing Machinery, 2019), 407–18, <https://doi.org/10.1145/3311927.3323136>.

⁶⁷ Reuben Binns et al., “Third Party Tracking in the Mobile Ecosystem,” in *Proceedings of the 10th ACM Conference on Web Science* (WebSci ’18: 10th ACM Conference on Web Science, Amsterdam Netherlands: ACM, 2018), 23–31, <https://doi.org/10.1145/3201064.3201089>; Jiaping Gui et al., “Truth in Advertising: The Hidden Cost of Mobile Ads for Software Developers,” in *Proceedings of the 37th International Conference on Software Engineering - Volume 1*, ICSE ’15 (Florence, Italy: IEEE Press, 2015), 100–110.

⁶⁸ Anirudh Ekambaranathan, Jun Zhao, and Max Van Kleek, “‘Money Makes the World Go around’: Identifying Barriers to Better Privacy in Children’s Apps From Developers’ Perspectives,” in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI ’21 (New York, NY, USA: Association for Computing Machinery, 2021), 1–15, <https://doi.org/10.1145/3411764.3445599>; Michael C. Grace et al., “Unsafe Exposure Analysis of Mobile In-App Advertisements,” in *Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks - WISEC ’12* (the fifth ACM conference, Tucson, Arizona, USA: ACM Press, 2012), 101, <https://doi.org/10.1145/2185448.2185464>; Theodore Book, Adam Pridgen, and Dan S. Wallach, “Longitudinal Analysis of Android Ad Library Permissions” (arXiv, April 18, 2013), <https://doi.org/10.48550/arXiv.1303.0857>.

⁶⁹ “Unity Announces Merger Agreement with IronSource,” Business Wire, July 13, 2022, <https://www.businesswire.com/news/home/20220713005473/en/Unity-Announces-Merger-Agreement-with-ironSource>.

⁷⁰ Amir Zaib Abbasi et al., “Do Pop-up Ads in Online Videogames Influence Children’s Inspired-to Behavior?,” *Young Consumers* 23, no. 3 (July 6, 2022): 362–81, <https://doi.org/10.1108/YC-06-2021-1347>.

⁷¹ Fitton and Read, “Creating a Framework to Support the Critical Consideration of Dark Design Aspects in Free-to-Play Apps.”

⁷² “Qustodio 2020 Annual Report on Children’s Digital Habits” (Charlotte, NC: Qustodio, 2020), [https://qweb.cdn.prismic.io/qweb/e59c2e0f-ef4f-4598-b330-10c430e2ec71_Qustodio+2020+Annual+Report+on+Child](https://qweb.cdn.prismic.io/qweb/e59c2e0f-ef4f-4598-b330-10c430e2ec71_Qustodio+2020+Annual+Report+on+Children%27s+Digital+Habits.pdf) ren%27s+Digital+Habits.pdf; “Ipsos MediaCT Tech Tracker Q4 2013” (London, UK: Ipsos MORI, 2013), https://www.ipsos.com/sites/default/files/publication/1970-01/IpsosMediaCT_Techtracker_Q4_2013.pdf.

already awash with children’s data⁷³ as the Commission’s 2019 settlement with YouTube and Google and 2021 settlement with OpenX further evidence.⁷⁴

Laying bare the difficulties facing developers, qualitative research with app developers has found that most developers understand that they have heightened responsibilities when developing apps for children.⁷⁵ However, they find that they do not have clear guidelines regarding application design, struggle to understand the complexities of the data economy that third-party libraries represent, and have few options. The only entities able to rein in these privacy threats are regulators like the Commission or the app marketplaces (e.g., Apple’s App Store, Google’s Play Store, Amazon’s Appstore).

Verifiable parental consent and age-assurance systems - a need for proportionality

The COPPA Rule’s methods for verifiable parental consent does not have a clearly articulated proportionate approach to collecting data for determining verifiable parental consent (VPC) and user age. The guidelines do not distinguish between information processing contexts and instead posit that any of the seven listed methods are suitable.⁷⁶ Without a proportionate approach, platforms and developers may collect highly detailed data (e.g., government IDs) for VPC and age-assurance purposes in low-risk processing environments. Age assurance systems are frequently touted in policy circles because of the significance of age in determining when a child can consent to information processing. While automating age assurance has the potential to better fit with how children use games and platforms, there is little impartial empirical evidence about their accuracy. There are multiple tiers to age assurance from self-declarations to age estimation (either via algorithm or via human) to verification based on document submissions. Inherent to age assurance is the collection of more data, and potentially quite sensitive data as in the case of age verification based on government-issued identification documents. A proportionate approach to age assurance and age-based restrictions is one potential option for rulemaking, akin to what is found in *The California Age-Appropriate Design Code*

⁷³ OECD, “Protecting Children Online: An Overview of Recent Developments in Legal Frameworks and Policies,” June 2, 2020, <https://doi.org/10.1787/9e0e49a9-en>.

⁷⁴ “Google and YouTube Will Pay Record \$170 Million for Alleged Violations of Children’s Privacy Law,” Federal Trade Commission, September 3, 2019, <https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law>; “Advertising Platform OpenX Will Pay \$2 Million for Collecting Personal Information from Children in Violation of Children’s Privacy Law,” Federal Trade Commission, December 14, 2021, <https://www.ftc.gov/news-events/news/press-releases/2021/12/advertising-platform-openx-will-pay-2-million-collecting-personal-information-children-violation>.

⁷⁵ Ekambaranathan, Zhao, and Van Kleek, “Money Makes the World Go Around.”

⁷⁶ 16 CFR § 312.5(b)

Act, OECD Recommendation on Children in the Digital Environment and the UK's Children's Code.⁷⁷ The level of assurance and the collection of associated data should be proportionate to the risk the information processing poses to children.

Right to erasure of data ("right to be forgotten")

COPPA permits the parents of children under 13 years of age to demand that their child's data be deleted. This is not enough to support children's informational self-determination and autonomy in the face of a "perpetual childhood" or the "end of forgetting".⁷⁸ Video games and digital media more broadly represent the first time that children are able to express themselves to a wide audience of individuals. Children have a public that goes beyond their family members, neighbors, and schoolmates. We recommend that the Commission fill a number of gaps regarding children's data deletion.

1. Allow for the deletion of all data collected before the age of 18.

COPPA only covers data from children under the age of 13 and at the parents' request. In light of the high levels of visibility of children on platforms along with their plasticity in their identities, they should be entitled to demand that any and all data collected before turning 18 be deleted. And this should be available to all individuals regardless of age. That is, a 25 year-old should be entitled to have their childhood data deleted.

2. Require businesses to notify users near their 18th birthday and inform them of their right to deletion.

Assuming that a right to deletion is made, requiring notification from companies to users that they have data about the user and that the user is entitled to have that data deleted will underpin the efficacy of the right. Children's data are processed by a seemingly endless number of companies.⁷⁹ Keeping track of each company throughout the course of one's childhood, especially given that parents frequently make decisions about data disclosure, is impossible. Conversely, it is much easier for companies to create automated notification processes for users approaching the age of 18 to inform them of their rights.

⁷⁷ The California Age-Appropriate Design Code Act.; Information Commissioner's Office, "Age Appropriate Design: A Code of Practice for Online Services: 1. Best Interests of the Child" (ICO, October 17, 2022), <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/1-best-interests-of-the-child/>; Organisation for Economic Co-operation and Development (OECD), "Recommendation of the Council on Children in the Digital Environment" (Paris, 2021), <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389>.

⁷⁸ Kate Eichhorn, *The End of Forgetting: Growing Up with Social Media* (Cambridge, MA: Harvard University Press, 2019).

⁷⁹ Barassi, *Child | Data | Citizen*.

3. Furnish children with the ability to delete data that their parent has posted about them.

COPPA does not regulate the processing of data that parents post about their children. This is a glaring omission with the advent of “sharenting”, the varied ways in which parents post information about their children on social media.⁸⁰ Children may disagree with the media about them posted by their parents.⁸¹ We note that posting about one’s children may be an important activity for parents and for this reason, encourage a balanced approach. Children, for example, could be entitled to have deleted particularly embarrassing or humiliating media about them posted by their parents. We moreover highlight that businesses may collect data about children posted by their parents with few safeguards due to COPPA’s scope being restricted to personal information collected directly from children under the age of 13.

Response to Question 17

Do techniques that manipulate consumers into prolonging online activity (e.g., video autoplay, infinite or endless scroll, quantified public popularity) facilitate commercial surveillance of children and teenagers? If so, how? In which circumstances, if any, are a company’s use of those techniques on children and teenagers an unfair practice? For example, is it an unfair or deceptive practice when a company uses these techniques despite evidence or research linking them to clinical depression, anxiety, eating disorders, or suicidal ideation among children and teenagers?

Yes. The more time spent on a platform, the more data can be collected. Platforms and developers can test their engagement strategies with great precision by working with detailed behavioral profiles of users. As we discuss more thoroughly in our response to **question 13**, children are frequently not aware of the complex data collection processes operating beneath the surface in games, free play is particularly important for children’s lives, and loot boxes (and other forms of gamblification) may pose risks to children. There is also a growing literature on the commercial exploitation of children in the digital environment, of which surveillance and prolonging online activity is a part.⁸² Games make liberal use of user-retention strategies that are common to many online services to usefully allocate resources, manage player numbers, pace the development and release of content. Player data is a necessary component of these systems, and they are designed to prolong engagement. As already discussed in our response to **question 14**, the business model of many games is premised on serving ads and/or facilitating in-game purchases. The more time spent within a game has the potential for more detailed behavioral profiles to be built based on in-game play and on engagement with ads.

⁸⁰ Stacey B. Steinberg, “Sharenting: Children’s Privacy in the Age of Social Media,” *Emory Law Journal* 66, no. 4 (2017 2016): 839–84.

⁸¹ Sonia Livingstone and Alicia Blum-Ross, *Parenting for a Digital Future: How Hopes and Fears about Technology Shape Children’s Lives* (Oxford: Oxford University Press, 2020).

⁸² Simone van der Hof et al., “The Child’s Right to Protection against Economic Exploitation in the Digital World,” *The International Journal of Children’s Rights* 28, no. 4 (December 14, 2020): 833–59, <https://doi.org/10.1163/15718182-28040003>; van der Hof et al., “Don’t Gamble With Children’s Rights’—How Behavioral Design Impacts the Right of Children to a Playful and Healthy Game Environment.”

Rules and their enforcement should focus on the surrounding context and pull from research findings that illustrate the contexts in which certain game designs may be deceptive or unfair. Interviews from mid-sized, UK-based game-development studios working on mobile games indicated that guidance from regulatory agencies would be valuable in their day-to-day operations.⁸³ Such guidelines “would help to orient ethical game design, ensure player protection, establish norms for online game communities, and de-risk development.”⁸⁴

Many games are designed to unnecessarily keep players engaged, which could be considered a “dark pattern”. The engagement is unnecessary because certain game features have no bearing on advancing in the game itself. Where games have users engage in repetitive and often tedious tasks, this is called “grinding”.⁸⁵ Children may be particularly susceptible to spending time grinding because of difficulties in assessing how much time is required for certain parts of a game.⁸⁶

Thinking beyond more straightforward surveillance tactics that rely on deceptive design, issues with user-generated content (UGC) sit at the intersection of privacy and intellectual property.⁸⁷ We encourage the Commission to treat UGC in a similar way as information disclosed in chats and other in-game communication technologies as we suggest in **question 13**. The COPPA Rule’s reliance on parental consent sits awkwardly with protecting user data from UGC because it may not be obvious to parents that their child will express themselves in a particular way with UGC.

In games such as Minecraft and Roblox, UGC is the core draw of the game - users can create sophisticated, playable worlds within the game itself. The privacy issue stems from the expressive nature of UGC: it can reflect a user’s interests, political leanings, or even sexual orientation. Games that facilitate UGC are important for children’s creativity and expression.⁸⁸ However, the data gathered from the UGC may be at odds with the child-creator’s interests. Such data can be mobilized for new product ideas, advertising strategies, and social profiling. Relying on UGC for commercial surveillance purposes is unfair and/or deceptive because the commercial subtext is obscured by the seemingly innocent pursuit of user engagement that seeks to create intimacy with young fan bases. Children’s creativity and play then ends up being repurposed for profit.

⁸³ Jayemanne et al., “Loot Boxes and Digital Gaming: A Rapid Evidence Assessment.”

⁸⁴ Jayemanne et al., 47.

⁸⁵ Arunesh Mathur, Mihir Kshirsagar, and Jonathan Mayer, “What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods,” in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI ’21 (New York, NY, USA: Association for Computing Machinery, 2021), 1–18, <https://doi.org/10.1145/3411764.3445610>.

⁸⁶ Zagal, Björk, and Lewis, “Dark Patterns in the Design of Games.”

⁸⁷ Grimes, *Digital Playgrounds*.

⁸⁸ Sara Grimes and Deborah A. Fields, “Children’s Media Making, but Not Sharing: The Potential and Limitations of Child-Specific DIY Media Websites,” *Media International Australia* 154, no. 1 (February 1, 2015): 112–22, <https://doi.org/10.1177/1329878X1515400114>; Grimes and Merriman, “‘Technically They’re Your Creations, but ...’: Children Making, Playing, and Negotiating User-Generated Content Games.”

Response to Question 18

To what extent should trade regulation rules distinguish between different age groups among children (e.g., 13 to 15, 16 to 17, etc.)?

Age-based distinctions are a commonplace and blunt instrument that do not robustly capture the nuances, diversities, and varying life circumstances of every young person. Yet, when regulating and setting content restrictions and standards for entire populations, age-based distinctions may be among the least bad options. We encourage the Commission to prioritize flexible and practicable rules that allow the unique circumstances and capacities of each child to be taken into account. If certain rules cannot be tailored to children's individual circumstances, then we encourage the Commission to ensure that age-based distinctions are designed to grant ever-greater autonomy to teens as they approach adulthood, rather than removing protections of their rights as minors who are still developing—physically, cognitively, and emotionally.⁸⁹

Flexibility could be achieved by specifying an age group, but then also creating a process by which a child with maturity 'beyond their years' can make additional decisions concerning their personal data. For example, this could be achieved by a capacity check that verifies the child understands the nature and purpose of the information processing and its reasonably foreseeable risks.⁹⁰ (Akin to capacity checks in clinical practice.) Such a process could be initiated with the parents' permission in light of legally recognized parental rights to decide many matters on behalf of their children.⁹¹ This has the potential to alleviate the common phenomenon of platforms closing their doors entirely to children.

As a general matter, we believe that the more justificatory work an age-based category does, the more well reasoned its usage should be. For example, in absence of a comprehensive federal data protection law that regulates the private sector, the differences in treatment of children's data under COPPA compared to that of teens are stark. Children under 13 benefit from myriad protections while those 13 and older are treated as adults. Such glaringly disparate treatment should be justified insofar as it is in the Commission's authority to regulate for other age groups when it comes to privacy matters.

If the age-based category is merely about the experience the child has on the platform (cf. whether or not any data protections apply at all), the stakes are still important, but less high. Ensuring children have experiences that are appropriate to their maturity is both a best practice within industry and in keeping with the provisions of the *Convention on the Rights of the Child*. Standards such as the Entertainment Software Rating Board (ESRB) content classification system, are widely used by

⁸⁹ Michael Freeman, "The Value and Values of Children's Rights," in *The Human Rights of Children: From Visions to Implementation*, ed. Antonella Invernizzi and Jane Williams (London: Routledge, 2011), 21–36, <https://doi.org/10.4324/9781315557007>; Gerison Lansdown, "The Evolving Capacities of the Child" (Florence: UNICEF Office of Research - Innocenti, 2005).

⁹⁰ Michael J. S. Beauvais et al., "Parental Access to Children's Raw Genomic Data in Canada: Legal Rights and Professional Responsibility," *Frontiers in Genetics* 12 (2021), <https://doi.org/10.3389/fgene.2021.535340>.

⁹¹ Anne C. Dailey and Laura A. Rosenbury, "The New Parental Rights," *Duke Law Journal* 71, no. 1 (2021): 75–166.

parents, teachers and others involved in gatekeeping/curating children’s access to tech, as well as by children and teens themselves in assessing the age appropriateness of new content and technologies.⁹² These categories are furthermore relied upon in *The California Age-Appropriate Design Code Act*, which divides children into the following age ranges: “0 to 5 years of age or “preliterate and early literacy”; 6 to 9 years of age or “core primary school years”; 10 to 12 years of age or “transition years”; 13 to 15 years of age or “early teens”; and 16 to 17 years of age or “approaching adulthood.””⁹³

Response to Question 19

Given the lack of clarity about the workings of commercial surveillance behind the screen or display, is parental consent an efficacious way of ensuring child online privacy? Which other protections or mechanisms, if any, should the Commission consider?

No. Parental consent *per se* is extremely limited and offloads too much responsibility onto parents.⁹⁴ To a certain extent, rules must assume that much activity is happening outside of the watchful eye of parents. Rules concerning commercial surveillance are more effective than asking each parent to understand commercial surveillance and how it affects their child on a case-by-case basis. In most circumstances, there will be some role for parents.

COPPA’s current notice parental requirements do not reasonably allow parents to exercise their responsibility to further their child’s best interests because the requirements are rooted in conveying technical information about the information processing without regard to the greater context. We encourage the Commission to adopt rules that require a robust disclosure of risks to parents for any matter in which they are being asked to make an informed choice.

We believe that parental consent is better suited to the bigger picture, less technical issues such as which games a child is playing, rather than the data collection practices each game presents. (Although, we also note that this sort of parental monitoring also has pitfalls.⁹⁵) Indeed, if parental consent were effective at securing children’s data, then most of the provisions of COPPA would be otiose because they deal with issues beyond parental consent such as purpose limitation and the release of personal information. That is to say, rules that protect children’s data irrespective of parental consent are immensely important.

⁹² Natalie Jomini Stroud and Ariel Chernin, “Video Games and the ESRB: An Evaluation of Parental Beliefs about the Rating System,” *Journal of Children and Media* 2, no. 1 (February 2008): 1–18, <https://doi.org/10.1080/17482790701733153>.

⁹³ The California Age-Appropriate Design Code Act., sec. 1(a).

⁹⁴ Lisa Archbold et al., “Adtech and Children’s Data Rights,” *University of New South Wales Law Journal* 44, no. 3 (2021): 857–77.

⁹⁵ William Balmford, Larissa Hjorth, and Ingrid Richardson, “Supervised Play: Intimate Surveillance and Children’s Mobile Media Usage,” in *The Routledge Companion to Digital Media and Children* (Routledge, 2020), 185–94.

Effective regulation of the digital environment must take into consideration the more robust agency children exercise online, which is frequently exercised outside of parents' watch. International approaches such as the United Nations Committee on the Rights of the Child's *General comment No. 25 (2021) on children's rights in relation to the digital environment* and the industry standard *IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children* take children's increased agency into account and focus on the design and underworkings of the digital environment. This approach furthermore coheres with scholarship on the need to adopt a consumer-protection approach to regulation that is grounded in how individuals actually interact with technologies.⁹⁶ Indeed, the Commission's own 2014 cases against Apple, Alphabet (Google), and Amazon concerning authorized purchases by minors on mobile platforms demonstrates the limitations of assumptions about parental consent and the watchful eye parents are supposedly exercising over their children.⁹⁷

Parental consent also requires authenticating parents and their relationships to their children. Doing so can be difficult and may in itself involve disproportionate data collection about the parent and child (not unlike the issues regarding age assurances we discuss in **question 14**). We also note the "passback" effect: many children use mobile devices that they do not own.⁹⁸ Children end up on multiple devices, which can make the management of authentication and permissions difficult.

If the Commission opines that more robust authentication procedures should underpin parental consent, it should craft guidance for industry about acceptable information requests from parents and children. A strict purpose-limitation principle should also be in place - no information given as part of parental authentication processes should be used for any other purposes.

We encourage the commission to keep an eye on the United Kingdom's Information Commission Office's (UK ICO) consultation on the Children's Code (Age-Appropriate Design Code). The UK

⁹⁶ Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Cambridge, Massachusetts: Harvard University Press, 2018).

⁹⁷ "Apple Inc. Will Provide Full Consumer Refunds of At Least \$32.5 Million to Settle FTC Complaint It Charged for Kids' In-App Purchases Without Parental Consent"; "Google to Refund Consumers at Least \$19 Million to Settle FTC Complaint It Unlawfully Billed Parents for Children's Unauthorized In-App Charges," Federal Trade Commission, September 4, 2014, <https://www.ftc.gov/news-events/news/press-releases/2014/09/google-refund-consumers-least-19-million-settle-ftc-complaint-it-unlawfully-billed-parents-childrens>; "FTC Alleges Amazon Unlawfully Billed Parents for Millions of Dollars in Children's Unauthorized In-App Charges," Federal Trade Commission, July 10, 2014, <https://www.ftc.gov/news-events/news/press-releases/2014/07/ftc-alleges-amazon-unlawfully-billed-parents-millions-dollars-childrens-unauthorized-app-charges>.

⁹⁸ Cynthia Chiong and Carly Shuler, "Learning: Is There an App for That? Investigations of Young Children's Usage and Learning with Mobile Devices and Apps" (New York: Joan Ganz Cooney Center at Sesame Workshop, 2010), <https://joanganzcooneycenter.org/publication/learning-is-there-an-app-for-that/>.

ICO is gathering evidence surrounding the implementation of the Code since it came into effect a year ago.⁹⁹

Response to Question 21

Should companies limit their uses of the information that they collect to the specific services for which children and teenagers or their parents sign up? Should new rules set out clear limits on personalized advertising to children and teenagers irrespective of parental consent? If so, on what basis? What harms stem from personalized advertising to children? What, if any, are the prevalent unfair or deceptive practices that result from personalized advertising to children and teenagers?

We encourage the Commission to pursue three options in order of preference: only permit contextual advertising for children’s platforms, develop standards for personalized advertising around the notion of the best interests of the child, or develop standards based around the notion of harm. Advertising plays an important role in funding the development of children’s video games and other media, but standards are needed. As we discuss in our response to **questions 13 and 14**, personalized nudges based on highly detailed data risks the economic exploitation of children and, perhaps more importantly, prematurely funneling a child’s nascent identity into specific categories for advertising purposes.

Should a ban on personalized advertising not be pursued (e.g., only allowing contextual advertising to children), new rules should set out clear limits on personalized advertising to children and teenagers irrespective of parental consent. We encourage the Commission to develop limits on personalized advertising that revolve around the best interests of the child standard or, in the alternative, a harm-based one. Such standards are needed because COPPA’s current approach to third-party disclosure (including advertising) is insufficient through its heavy reliance on parental consent to ensure children’s best interests are furthered (see also our response to **question 19**). Age-appropriate design codes and industry standards already make use of the concept to underscore that businesses should be held to higher standards with respect to children’s data and experiences.¹⁰⁰ Determining a child’s best interests for advertising should consider similar factors as those the Information Commissioner Office lists in the Age-Appropriate Design Code: safety from exploitation; health and wellbeing; physical, psychological, and emotional development; development of identity and viewpoints; right to freedom of association and play; the role of parents in promoting a child’s best interests; and, the evolving capacity for a child to have a say in a matter.

⁹⁹ “ICO Consultation: Children’s Code Evaluation” (ICO, November 19, 2022),

<https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-childrens-code-evaluation/>.

¹⁰⁰ Information Commissioner’s Office, “Age Appropriate Design: A Code of Practice for Online Services: 1. Best Interests of the Child”; “IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children,” *IEEE Std 2089-2021*, November 30, 2021, 1–54, <https://doi.org/10.1109/IEEESTD.2021.9627644>.

If a harm-based standard is pursued, we believe that inspiration for types of harms may be drawn from the proposed *Kids Online Safety Act*, which focuses on harms such as “the promotion of self-harm, suicide, and eating disorders; patterns of use that show or encourage addiction-like behavior; sexual exploitation; physical harm, online bullying, and harassment of a minor; promotion and advertisement of products or services that are unlawful for minors; and predatory marketing practices”.¹⁰¹ Additional guidance may be drawn from the UN Committee on the Rights of the Child’s *General comment No. 25 (2021) on children’s rights in relation to the digital environment* on commercial advertising and marketing, which flags the use of “advertising design features that anticipate and guide a child’s actions towards more extreme content” as a harm of commercial surveillance.¹⁰²

Finally, we recall our response to **question 14** regarding third-party application libraries: smaller and mid-sized game developers can have difficulty navigating the landscape of monetization tools offered by advertising networks, despite their desire to uphold children’s best interests.¹⁰³ Other research also suggests that third-party libraries are frequently to blame for COPPA violations.¹⁰⁴ We believe the Commission should formulate disclosure requirements for providers of third-party libraries to better specify responsibilities and facilitate smaller game developers’ compliance with any applicable advertising rules. We furthermore encourage the Commission to liaise with the U.S. Small Business Administration to determine the potential for complementary strategies that raise the standards for children’s best interests, privacy and well-being, while supporting small businesses.

Response to Question 22

Should new rules impose differing obligations to protect information collected from children depending on the risks of the particular collection practices?

Yes. We encourage the Commission to develop a proportional, risk-based approach to its rules on commercial surveillance and data security. Coarse location data to determine a child’s city or town for serving ads related to a concert coming to that location (for instance) poses fewer risks than using a combination of physiological and behavioral data to extend a child’s screen time. Such rules should ensure that obligations and safeguards are proportionate to the risks the particular collection practices and processing operations pose. (This is similar to the approach we suggest in our response to **question 14** regarding VPC and age-assurance systems.) This would mean that low-risk collection and processing is subject to less onerous requirements than high-risk collection and processing. Risk-based

¹⁰¹ Richard Blumenthal and Marsha Blackburn, “S.3663 - 117th Congress (2021-2022): Kids Online Safety Act,” July 27, 2022, 2021/2022, <https://www.congress.gov/bill/117th-congress/senate-bill/3663>.

¹⁰² United Nations Committee on the Rights of the Child, “General Comment No. 25 (2021) on Children’s Rights in Relation to the Digital Environment” (United Nations Committee on the Rights of the Child, March 2, 2021), para. 40, CRC/C/GC/25.

¹⁰³ Jayemanne et al., “Loot Boxes and Digital Gaming: A Rapid Evidence Assessment.”

¹⁰⁴ Irwin Reyes et al., “Won’t Somebody Think of the Children? Examining COPPA Compliance at Scale,” *Proceedings on Privacy Enhancing Technologies*, 2018, <https://petsymposium.org/popets/2018/popets-2018-0021.php>.

approaches are already widespread in data protection practice.¹⁰⁵ The advantage of taking a risk-based approach is that it is flexible - companies can design their data collection and processing operations and commercial surveillance practices more generally to reduce risks to children. It also allows for innovative, privacy-preserving data analysis techniques such as differential privacy, homomorphic encryption, and federated learning to be used if the conditions allow.¹⁰⁶

To ensure effectiveness of such an approach, we recommend rules that require the appointment of a children’s privacy officer (CPO) in every company. Taking inspiration from the GDPR’s requirement of a data protection officer, the CPO should be responsible for understanding the interface of the company’s business practices with children’s privacy rules. The Commission could support such a role through developing privacy impact assessment templates that are designed from the perspective of the child’s rights and best interests. The UK ICO already has developed templates for game developers to help them identify issues in the design and development of their gaming applications.¹⁰⁷ We also believe the Commission should consider either adopting or adapting children’s rights impact assessments (CRIAs) for either its own rulemaking or its business guidance. CRIAs allow decision-makers to systematically consider how their activities and decisions affect children’s rights and interests. They have received growing attention in responding to challenges of securing children’s rights in the digital environment.¹⁰⁸

¹⁰⁵ Raphael Gellert, “We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-Based Approaches to Data Protection,” *European Data Protection Law Review (EDPL)* 2, no. 4 (2016): 481–92; Raphaël Gellert, “Understanding the Notion of Risk in the General Data Protection Regulation,” *Computer Law & Security Review* 34, no. 2 (April 1, 2018): 279–88, <https://doi.org/10.1016/j.clsr.2017.12.003>.

¹⁰⁶ Lidia Dutkiewicz et al., “Privacy-Preserving Techniques for Trustworthy Data Sharing: Opportunities and Challenges for Future Research,” in *Data Spaces : Design, Deployment and Future Directions*, ed. Edward Curry, Simon Scerri, and Tuomo Tuikka (Cham: Springer International Publishing, 2022), 319–35, https://doi.org/10.1007/978-3-030-98636-0_15.

¹⁰⁷ “Sample Data Protection Impact Assessment: Mobile Gaming App” (ICO, August 12, 2022), <https://ico.org.uk/for-organisations/childrens-code-hub/sample-data-protection-impact-assessment-mobile-gaming-app/>.

¹⁰⁸ Pratik Mukherjee, Kruakae Pothong, and Sonia Livingstone, “Child Rights Impact Assessment: A Tool to Realise Child Rights in the Digital Environment” (London: 5Rights Foundation, March 2021), <https://digitalfuturescommission.org.uk/wp-content/uploads/2021/04/CRIA-Report-revised-final.pdf>.