March 31, 2021

Data Protection Commission
Children's Policy Unit
21 Fitzwilliam Square South
D02 RD28, Ireland

RE: Children's Consultation

Common Sense is an independent, not-for-profit organisation dedicated to helping children and families thrive in a rapidly changing digital world. We are based in San Francisco, with offices across the United States and in the United Kingdom. We are a leading organization that parents, teachers, and policymakers go to for unbiased information, trusted advice, and innovative tools to harness the power of media and technology as a positive force in all children's lives.

Since launching 15 years ago, Common Sense has helped millions of children and families think critically and make smart, responsible choices about the media they create and consume. Common Sense reaches 125 million households and our award winning Digital Citizenship Curriculum is the most comprehensive K-12 offering of its kind in the education field; we have over 1 million registered educators using our curriculum representing over half of schools in the U.S. And just this year, we launched a UK Digital Citizenship Curriculum. Common Sense champions policy solutions that put children first, working with policymakers and companies to craft rules and best practices that protect privacy, improve digital equity and connectivity, and promote the digital well-being of children and families.

Common Sense applauds the Data Protection Commission (DPC) for its efforts to support and protect children online through its draft Fundamentals for a Child-Oriented Approach to Data Processing (Fundamentals). The Fundamentals embody many of the principles and practices Common Sense has highlighted in debates on privacy and data protection in the U.S., and the principles and guidance in the Fundamentals will help encourage organizations to design products and services with privacy, digital well-being, and the best interests of the child in mind and from the start.

The privacy interests of children are under siege. As the United Nations Children's Fund (UNICEF) recognizes, "the sheer volume of digital information that is generated during the first 18 years of life, and the multiple and advancing technological means for processing children's data all raise serious questions about how children's right to privacy can best be preserved and protected."[1] Common Sense believes that companies must empower young people, and parents, to make better decisions online. Because we know, as does the DPC, that privacy matters for young people and

[1] United Nations Children's Fund (UNICEF), Industry Toolkit: Children's Online Privacy and Freedom of Expression (2018), *available at* https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf.

families.[2] We believe companies should be transparent with families about their privacy and security practices, minimize personal information collection and retention, and appropriately safeguard any personal information they do collect. We are pleased to offer comments in response to the consultation on the draft Fundamentals.

Overall, we are greatly encouraged by the Fundamentals. We particularly appreciate the focus on the fundamental rights and best interests of children, and the notion that "consent doesn't change childhood" and cannot be used as the basis for children losing their rights or for dictating when a child can access a service.[3] In the U.S., unfortunately, we have seen companies misinterpret the Children's Online Privacy Protection Act (COPPA) and act as if once they get consent they are free to do whatever they wish (and, unfortunately, such behavior is rarely the subject of enforcement). We also see companies use COPPA compliance as an excuse to cut off younger children. Thus, we are grateful to the DPC for being very clear that such behavior is inappropriate in the Fundamentals.

We also appreciate the recognition that certain practices, like targeted advertisements, are simply inappropriate for children -- we believe that certain profiling activities, particularly commercial profiling used to target advertisements, are never in the best interests of a child. Indeed, in the U.S., we have pressed for legislation that would flatly prohibit behaviorally targeted advertisements to children, as well as profiling based on race, ethnicity or proxies thereof.[4] Additionally, we agree that sites which are uncertain about their audience would do best to implement privacy-protective behaviors across the board, and the better practice is to provide protections from the start and enable adults to opt out if they so choose.

Our comments propose some suggestions to further clarify and strengthen the draft Fundamentals, including: detailing detrimental design practices, providing more guidance as to what constitutes appropriate data minimisation and data sharing, and further confirming a risk-based, evolving, and privacy-protective age verification approach. In addition, we suggest that future Codes of Conduct consider questions of content moderation and amplification, which are inextricably linked to privacy.

---

[2] *See* Common Sense Media, Privacy Matters: Protecting Digital Privacy for Parents and Kids (2019), *available at* https://www.commonsensemedia.org/sites/default/files/uploads/kids_action/csm_privacymatters_protecting_digital_privacy_1.pdf.

[3] Data Protection Commission, Draft Fundamentals for a Child-Oriented Approach to Data Processing, at 7 [hereinafter Fundamentals].

[4] Ariel Fox Johnson, *Improving COPPA: A Road Map for Protecting Kids' Privacy in 2020 and Beyond*, Common Sense Media (29 Jan. 2020), https://www.commonsensemedia.org/kids-action/blog/improving-coppa-a-road-map-for-protecting-kids-privacy-in-2020-and-beyond.

I. Further Elaborating Data Protection By Design and Default

A. Manipulative Design and Nudge Techniques

The Fundamentals provide an excellent guide to entities looking to place children's rights first. Some of this guidance, however, could be further elaborated, particularly that found in Section 7.3, including detailing detrimental uses and what constitutes manipulative design and appropriate data minimisation.

Providing additional guidance and explanations about what types of data processing are detrimental and not in the best interests of children will help clarify what nudge techniques and data minimisation are appropriate. Detrimental uses must capture and encompass how technologies impact children's social, emotional, cognitive, and physical development. Because research on the effects of media and technology on children's well-being is limited, we expect what is deemed detrimental may change in the future. The DPC acknowledges that the draft Fundamentals are designed to be consistent with the UK Age Appropriate Design Code (AADC) and that the principle of placing the best interests of the child underpins both efforts.[5] We believe the AADC's specific discussion of detrimental uses of data and nudge techniques is useful and could be incorporated into the Fundamentals.[6] In addition, addressing such design tactics would be consistent with proposed bipartisan legislation in the U.S. addressing dark patterns that subvert user autonomy and promote compulsive usage in children.[7]

Nudges, dark patterns, and other types of manipulative design facilitate detrimental uses of data and undermine children's fundamental rights and best interests. Dark patterns are user interfaces that trick, subvert, or confuse users, make it difficult for users to express their actual preferences, or manipulate users into taking certain actions.[8] Companies build user interfaces using dark patterns that employ techniques based on extensive behavioral psychology research and often mislead users into agreeing to settings or practices. While adults fall prey to these techniques, children are especially vulnerable to platforms that employ dark patterns and could unknowingly make purchases, divulge information, or agree to exploitative settings (which is inconsistent with any notion of informed consent).

---

[5] Fundamentals at 3.
[6] UK ICO Age Appropriate Design Code, Standard 5: Detrimental Use of Data (2020), https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/5-detrimental-use-of-data/.
[7] Deceptive Experiences To Online Users Reduction (DETOUR) Act, S. 1084 (2019-2020), https://www.congress.gov/bill/116th-congress/senate-bill/1084/all-info.
[8] Jamie Luguri & Lior Jacob Strahilevitz, Shining a Light on Dark Patterns (2019), *available at* https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/shining-a-light-on-dark-patterns.pdf.

We believe that such practices have a largely detrimental and harmful effect on youth,[9] and encourage a formal position stating so. The draft Fundamentals suggest that companies avoid the use of nudge techniques, but the DPC should further address manipulative design and its impact on children. For one, companies have regularly been accused of deploying dark patterns to circumvent and undermine privacy rules under the GDPR.[10] Research from the Norwegian Consumer Council has demonstrated how tech companies have continued to use dark patterns and other interface design features meant to manipulate users, nudging users towards privacy intrusive options.[11] More recently, the French data protection authority (CNIL) stressed how important design is to protect privacy, stating that "using and abusing a strategy to divert attention or dark patterns can lead to invalidating consent."[12]

We recognize that the Fundamentals are focused on children's data protection considerations, but the use and deployment of dark patterns extends beyond privacy to how children use online apps and services. They can also be used to compel usage and purchases, for example. In our conversations with children, they report feeling great anxiety over going on vacation and not being able to keep up with "Snap streaks" or of having designated offline time in the evening and not being able to respond immediately to friends' postings on social media. Teens in our studies report they feel "addicted" to technology . These tech features create a sense of immediacy and an "always on" feeling in children, and are designed to subvert user autonomy and choice and cultivate compulsive usage. Oftentimes games will use beloved characters or hosts to shame children into purchase or extended gameplay. Games also create confusing interfaces where it's hard for children to discern the difference between content and advertising or a link to make a purchase. Platforms that automatically extend viewing by serving up unrequested content, sometimes even before the requested content is concluded, can trap families into extended viewing sessions. In some cases, designers engineer games with artificial difficulty curves to induce children to spend money on upgrades simply to progress. These games are often offered for free, enticing players to download and even offering them a false sense of progression upon initial download before artificially increasing difficulty to induce compulsive purchases.

---

[9] Subcommittee on Consumer Protection and Commerce of the House Committee on Energy and Commerce hearing on "Kids Online During COVID: Child Safety in an Increasingly Digital Age" (11 Mar. 2021), *available at* https://energycommerce.house.gov/committee-activity/hearings/hearing-on-kids-online-during-covid-child-safety-in-an-increasingly.

[10] Lilly Smith, *Why you can't escape dark patterns*, Fast Company(7 Feb. 2020, https://www.fastcompany.com/90452333/why-you-still-cant-escape-dark-patterns; Karl Bode, *Companies Use 'Dark Patterns' to Mislead Users About Privacy Law, Study Shows*, Motherboard Vice (13 Jan. 2020), https://www.vice.com/en/article/g5xg74/companies-use-dark-patterns-to-mislead-users-about-privacy-law-study-shows.

[11] Norwegian Consumer Council, Report: Deceived by design (27 June 2018), https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/.

[12] CNIL, Shaping Choices in the Digital World: From dark patterns to data protection: the influence of ux/ui design on user empowerment (Jan. 2019), *available at* https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf.

Ultimately, digital platforms collect and process data with the prime goal of increasing user engagement,[13] and manipulative design supports this. We encourage the Fundamentals to more formally state that this is detrimental to children and further detail what practices are problematic.

B. Data Minimisation and Data Sharing

Relatedly, we appreciate that the Fundamentals support data minimisation. We believe this guidance could be further fleshed out, including a clear statement that data minimisation for children should include collecting, maintaining, or sharing only what is needed to provide a service. In addition, here or in subsequent industry-specific codes of conduct, we believe it would be useful to provide examples of compliance with data minimisation (such as reducing the level of granularity of information collected).

We agree with the Fundamentals that data sharing and visibility of children's information is something companies should take care to limit. This is another recommended measure that we believe could be more clearly stated and given some additional scope. The Fundamentals indicate that one should not "systematically share a child's personal data . . . without clear parental knowledge, awareness, and control" or "the opportunity for intervention."[14] We support this, particularly for young children, as it is critical parents understand and can act on what a company may wish to do. We believe this requirement should more definitively include consent, either parental consent if appropriate or a child's own consent. And additionally we believe that sharing should not occur without a compelling reason, taking into account the best interests of the child, as required under the AADC.[15] If there is no compelling reason, and no consent, a company should not be sharing personal data, whether or not it has provided an "opportunity for intervention".

In addition, we think that further discussion may be warranted for situations where parental involvement and awareness are less appropriate, but rather should be replaced by a teenager's own involvement, awareness, and consent. (The requirement of a compelling reason to share will also provide additional safeguards here.) Enabling such decisionmaking on the part of the child themselves is particularly important for older teens whose parents may be less appropriately and understandably involved in their online decisions and activities, and is consistent with a recognition of evolving capacities as well as legislation we have supported in the U.S. that would enable teenagers past the age of "digital consent" to make their own supported and informed choices.[16]

---

[13] Karen Hao, *How Facebook got addicted to spreading misinformation*, MIT Tech Review (11 Mar. 2021), https://www.technologyreview.com/2021/03/11/1020600/facebook-responsible-ai-misinformation/.
[14] Fundamentals at 60.
[15] UK ICO Age Appropriate Design Code, Standard 9: Data Sharing (2020), https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/9-data-sharing/.
[16] Johnson, *supra* note 4.

II. Age Verification Guidance

Common Sense agrees with the DPC's position that digital services should provide a strong "floor" of protection for all users, or deploy a risk-based approach to age verification. This approach allows adults to opt out of protections and reduces incentives for children to lie about their ages. As the DPC acknowledges, we believe "reasonable efforts" should vary depending upon the type of service and the impact it is likely to have on a user's fundamental rights, including rights to privacy and data protection. Sites that pose little risk to children should be able to use simpler mechanisms, which can enable adults to more easily "opt out" of the protective defaults. We would also caution against requiring or promoting government IDs as a primary type of age verification; that form of age verification can be privacy invasive as well as circumventable by a child.

We appreciate that the draft Fundamentals recognizes that age verification tools are a developing area, and there is much innovation occurring in this space. The DPC notes that age verification mechanisms should be reviewed in light of emerging technologies and efficacy assessments that rely on user testing and subject matter experts.[17] We note that the DPC briefly discusses some of the methods for obtaining verifiable parental consent under COPPA, but the DPC may also want to encourage further research in this space. The UK ICO, for instance, has launched a regulatory "sandbox" that includes projects to ensure children can explore the internet safely, including novel age estimation software and other AADC tools.[18]

III. Future Work on Codes of Conduct: Community Guidelines and Content Amplification

One area for future work in Codes of Conduct would be to address adherence to platform policies and community standards. The AADC explicitly requires that companies adhere to their published terms and conditions *and* actively uphold and enforce those rules and conditions.[19] Common Sense believes, at minimum, that companies must be held accountable to their written promises, including community guidelines and other policy pronouncements about content, tools, and other protections for individuals. Data protection increasingly intersects with these policy issues involving content moderation and platform accountability. The proposed Digital Services Act will implicate data protection obligations under the GDPR and Irish data protection law.

The DPC's views on this are important because policy measures to address inappropriate content and harmful interactions online can both implicate privacy concerns--such as the use of data to amplify or target harmful content or manipulate users--and come into tension with privacy

[17] Fundamentals at 41.
[18] Press Release, ICO supports projects to strengthen children's privacy rights (15 Jan. 2021), https://ico-newsroom.prgloo.com/news/ico-supports-projects-to-strengthen-childrens-privacy-rights.
[19] UK ICO Age Appropriate Design Code, Standard 6: Policies and Community Standards (2020), https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/6-policies-and-community-standards/.

protection.[20] For example, discreet monitoring undermines trust, and as Common Sense has recommended, safeguards that encourage open dialogue are more likely to be helpful.[21] Considering, in future Codes, clear rules for online platforms with respect to complying with their written promises, transparency in content moderation, and addressing amplification of harmful-but-legal content would be helpful in protecting and supporting children's fundamental rights. And they are in line with proposals Common Sense has supported in the US, such as the Kids Internet Design and Safety (KIDS) Act, which would establish rules for online platforms with respect to advertising targeted toward children and curb the use of manipulative design that amplifies inappropriate content, including (1) sexual material, (2) violence and cyberbullying, (3) adult activities, and (4) other dangerous and exploitative content.[22]

--

Thank you again for the opportunity to provide feedback on the Fundamentals. We are very appreciative of the DPC's work in this area and outreach to all stakeholders, and we hope to be a resource as future Codes are developed.

Respectfully submitted,

[redacted]

[20] Joseph Jerome, Safe and Secure VR: Policy Issues Impacting Kids' Use of Immersive Tech, Common Sense (Mar. 2021), *available at* https://d2e111jq13me73.cloudfront.net/sites/default/files/uploads/safe_and_secure_vr_policy_issues_impacting_kids_final.pdf.
[21] Caroline Knorr, *Parents' Ultimate Guide to Parental Controls*, Common Sense Media (9 Mar. 2021), https://www.commonsensemedia.org/blog/parents-ultimate-guide-to-parental-controls.
[22] Press Release, Introduction of the Kids Internet Design and Safety (KIDS) Act (5 Mar. 2020), https://www.markey.senate.gov/news/press-releases/senators-markey-and-blumenthal-introduce-first-of-its-kind-legislation-to-protect-children-online-from-harmful-content-design-features .