5RIGHTS FOUNDATION

Dear Elizabeth Denham,

Systemic breaches of the Age Appropriate Design Code

It has been very heart-warming to see the changes that have been announced by multiple companies during the Code transition period. The ambition behind the Code was to impact the lived experiences of children and many of the changes we are seeing, from reductions in targeted advertising to higher default privacy settings, will make the digital world safer and more enjoyable for young people. I want to recognise the efforts made by the many businesses and organisations that have complied with the Code and thank you and your team for their tireless efforts during the transition period and for all the guidance and support they have made available.

While it is important to celebrate changes that have been made, I am writing to raise three areas of concern that the ICO should review as a matter of urgency.

1. The announcements from companies that have already made changes to their services show a great disparity in approaches to compliance. Whilst I am supportive of different companies taking the approach that is most effective for them, compliance must not become a 'pick and mix'. It would be helpful for the ICO to consider the changes services have made in relation to direct messaging, high privacy, extended use, targeted advertising, and offer a clear opinion about establishing what is adequate and what is best practice, to drive compliance to a level that will protect children.
2. The technology market is made up of different products and services: search, social media, games, e-commerce, EdTech etc. It is clear from the announcements and changes, or lack thereof, that some companies are not taking sufficient action to meet the Code. The Code is ground-breaking in many ways, most notably for the way it is shaped around the child. Any product or service "likely to be accessed" by a child is in scope and there should be no free pass for those that are cynically hiding behind others. With that in mind, I would ask that the ICO look at gaming companies to ensure their services meet the standards of the Code.
3. There is a danger that the Code is being interpreted as introducing a handful of safety measures, rather than a requiring a holistic re-design of the systems and processes of services to ensure their data collection practices are in the best interests of children. If the Code is to have real value in protecting children's safety and rights in the digital environment, the ICO must make sure that it is respected in practice.

In July and August 2021, 5Rights conducted extensive research, testing products and services to identify gaps in compliance with the standards set out in the Code. Our methodology for undertaking this research is set out in Appendix C. Below is a summary of 12 common issues we identified that are indicative of widespread breaches of the Code across the tech sector. Appendix A highlights the systemic nature of these breaches and draws attention to the multiple companies that appear to be failing to comply in the same or similar ways.

We understand that some companies and organisations will have brought in last minute changes to ensure compliance with the 2nd September deadline and may rightly be able to show additional protections, and we welcome any changes for the better. But the systemic nature of the problems we have unearthed leads us to believe that, in many cases, these problems are likely to persist. We also recognise that there are and will be many more breaches than those we have identified, and it is our hope that the ICO will investigate the systemic nature of these

apparent breaches and publish guidance to set out expectations for all companies on these matters.

It is not our intention at this point to make any individual complaint but hope that by identifying a number of thematic issues, it will clarify the ICO's formal position on common issues which will facilitate compliance action in the future. The Code provides a golden opportunity to make clear what steps business must take to protect children's right to privacy and data protection, backed up by a strong regulatory framework. We hope that our research will assist the ICO to ensure that the Code marks a transformation in children's experience of the digital world.

The research was conducted ahead of the revelations from the Facebook whistleblower, Frances Haugen. We consider them to be relevant and welcome the ICO's statement that they are monitoring details from Haugen's testimony and considering the information in relation to the Code.

Yours sincerely,

Baroness Kidron
Chair, 5Rights Foundation

Summary of systemic breaches

Note: Many of the breaches contravene more than one standard in the Code and many fail to meet transparency requirements (standard 4). All the data practices set out below are not "in the best interests of the child" (standard 1).

1. **Insufficient age assurance** (standard 3 – age appropriate application)

Many services with age restrictions can be easily accessed by children under the minimum age of use, including adult-only services. In addition, some services state that they do not collect any personal data from children but in many cases these services do not have any form of age assurance or they use age assurance that can be easily bypassed. If these services do not identify child users, it is unclear how they are upholding their own privacy policies or are able to implement the Code.

2. **The minimum ages of use for games and apps are mis-advertised on app stores** (standard 3 – age appropriate application)

Many services with age restrictions are advertised on the Apple App and Google Play stores as child-friendly, suitable for users of any age or ages younger than those specified in the service's published terms. The app stores also allow accounts registered as children to download age-restricted apps with little or no friction.

3. **Use of data creates content, conduct and contact risks** (standard 5 – detrimental use of data, standard 6 – policies and community standards, standard 10 – geolocation and standard 12 – profiling)

Data-driven features create content, contact and conduct risks to children. These include recommendation systems that serve up detrimental material and friend or follower suggestions that connect children with adult strangers.

4. **Failure to enforce community standards** (standard 6 – policies and community standards)

Services routinely fail to enforce their community standards. Many rely on users to report content or activities that violate community rules in place of proactive moderation.

5. **Use of dark patterns and nudges** (standard 7 – default settings, standard 10 – geolocation and standard 13 – nudge techniques)

Many services use dark patterns and nudges to encourage users to take certain courses of action, including lowering their privacy setting and sharing their location. Nudges which encourage children to lower high privacy default settings undermine compliance with the default settings standard of the Code.

6. **Age-inappropriate financial pressures** (standard 5 – detrimental use of data and standard 13 – nudge techniques)

Many 'freemium' services put inappropriate contractual or financial pressure on child users. These include exhortations to purchase in-game items, in-game 'rewards' designed to incentivise more frequent and extended use, aggressive 'pay walls' and 'limited-time' features that introduce a sense of artificial scarcity. In some cases, these practices contravene external guidance referred to in the Code, including the Office of Fair Trading's principles for online and app-based games (now under the Competition and Markets Authority).

7. **Low default privacy settings** (standard 7 – default settings, standard 9 – data sharing and standard 13 – nudge techniques)

Low default privacy settings put children at risk of being visible, identifiable and contactable by strangers, while allowing services to maximise the amount of data they can collect from children.

8. **Excessive data sharing with third parties** (standard 9 – data sharing)

Many services ask users to consent to their data being shared with third parties. Others make reference to third parties without being fully transparent with users about the nature or scale of data sharing. These third parties very often go on to share user data with their own partners, who may go on to share with their partners. As such, users signing up to a single service may have their data shared with an endless chain of third parties.

9. **Lack of transparency and excessive data sharing between services and third party login providers** (standard 4 – transparency, standard 7 – default settings, standard 8 – data minimisation and standard 9 – data sharing)

Many products and services allow users to register or sign in via existing accounts they have with other providers, such as Google, Apple, Facebook, Snapchat or TikTok. Some providers make it difficult or even impossible to register or log in via other means. It is often unclear what information is shared between the service and the third party log in/authentication provider.

10. **Published terms are not age-appropriate** (standard 4 – transparency)

Most services do not have age-appropriate published terms. Terms are sometimes impossible to find or revisit past the point of registration or initial access. Among those services investigated, only a handful provided summaries of their policies or offered any age-appropriate alternatives.

11. **Insufficient tools to exercise data rights** (standard 15 – online tools)

Few apps provide all of the online tools required by the Code. In many cases, reporting tools are not highlighted at any stage during the set-up/registration process and tools for downloading personal data are often not available.

12. **Connected devices** (standard 4 – transparency and standard 14 – connected toys and devices)

Connected devices, and the providers of apps built for them, very often fail to provide an accessible privacy policy or mechanism for children to understand how their data is used.