Written evidence submitted by the End Surveillance Advertising to Kids coalition - 5Rights Foundation, Andrew Simms, New Weather Institute, Avaaz, Dr Elly Hanson, Fairplay, Foxglove Legal, Global Action Plan, Global Witness, New Economics Foundation, The Mission and Public Affairs Council of the Church of England (OSB0150)

1. Introduction

The *End Surveillance Advertising to Kids* coalition brings together organisations calling for government action to protect children from surveillance advertising.

"Surveillance advertising" (also sometimes called "targeted advertising", "micro-targeting", or "behavioural advertising") relies on large-scale data collection and behavioural profiling, to present users with highly personalised adverts. Children are less able to understand these advertising practices and are especially vulnerable to being manipulated by such adverts.

Our recent report, produced by the New Economics Foundation, set out in detail why, and how, the government should act to address the harms associated with surveillance advertising for kids.

We are grateful for the opportunity to submit evidence to your committee. Our submission focuses on answering the following 3 questions from your Call for Evidence:

- Are children effectively protected from harmful activity and content under the measures proposed in the draft Bill?
- Does the Bill deliver the intention to focus on systems and processes rather than content, and is this an effective approach for moderating content? What role do you see for e.g. safety by design, algorithmic recommendations, minimum standards, default settings?
- Are there any types of content omitted from the scope of the Bill that you consider significant e.g. commercial pornography or the promotion of financial scams? How should they be covered if so?

As a coalition we believe large social media companies are currently under-regulated. Decisions about the design and operation of large digital spaces have big implications for society and for individual wellbeing - yet they are currently left entirely to the companies, and made in the interests of shareholders and advertisers. The draft Bill is an opportunity to step away from this failed self-regulation. Our specific criticisms of the draft Bill should be seen in the context of our overall support for improved regulation in this area.

Our concerns about the draft Bill's silence on surveillance advertising, and how this weakens its ability to drive improvements in the safety of platforms' design, systems and processes, could be summarised as follows:

1. **Surveillance advertising is the business model which drives platforms' decisions about design, systems and processes.** We are concerned that any regulatory regime that fails to address this business model will struggle to deliver safer design or safer systems.

2. **Surveillance advertising to kids is a harmful type of content in and of itself.** It is not currently regulated effectively, and the draft Bill's exemptions for all paid-for advertising content therefore leave huge gaps in its provisions regarding harmful content.

This submission explains why we consider surveillance advertising to kids to be a major problem which an effective online safety regulatory regime needs to tackle-head on. We then make some suggestions for how the government could begin to tackle this, and explain why we think it makes sense for this to be done within the Online Safety Bill.

2. Surveillance advertising is a business model which drives platforms' decisions and fuels online harms to children

Platforms' current designs, systems and processes have all been developed to serve a surveillance advertising business model. This business model is associated with a broad range of online harms, but as a coalition we are particularly concerned about the impact this business model has on platforms' approach to protecting children's safety and wellbeing.

The surveillance advertising business model requires the large-scale collection, profiling, and sharing of children's personal information and online behaviour. It incentivises design choices which maximise the amount of user data which can be harvested for behavioural profiling, and recommender algorithms which maximise "engagement" - i.e. time spent on the platform, to generate data and view ads - to the detriment of all other considerations.

The results have been unhealthy online spaces which fail to keep children safe. As the 5Rights Foundation observes:

> *"There is not a single online harm or socio-digital problem that is not made worse by micro-targeting. Disinformation is more destructive when targeted at the people most likely to believe or act on it. Elections are less free, fair, and transparent when the information received by one voter is different to and/or concealed from another. Polarisation is deepened by filter bubbles that entrench our biases, reduce our capacity for empathy, and even constrain our freedom of thought. Pro-suicide, self-harm, or eating disorder content is far more dangerous when served up automatically, proactively, and repeatedly by the recommender systems of platforms popular with young people. Enabling businesses to communicate more persuasively with their customers cannot outweigh the risks to children that the whole surveillance advertising system poses."*

The draft Bill fails to recognise this profound tension between the imperatives of the surveillance advertising business model, and the development of digital environments which are safe and healthy for children.

The closest the draft Bill gets is a provision (s61(6)) that Ofcom includes consideration of "characteristics", including a platform's "business model", in its risk assessments and risk profiles. This provision appears weak. It is not clear how Ofcom can challenge a platform's

own risk assessments, or the role which a platform's business model plays in its decision-making.

The draft Bill's "children's risk assessment duty" rightly requires platforms to consider "functionalities of the service facilitating the presence or dissemination of content that is harmful to children" (section 9(d)). However, given the exemption for paid-for content (section39(2)(f)), and the failure to specify advertising functionalities amongst the "functionalities that present higher levels of risk", it seems likely that platforms will choose not to include assessment of the risk of advertising functionalities. It would be hard to describe as comprehensive a risk assessment that fails to consider the risks associated with offering the ability to profile and target children with advertising content, at scale, to any individual adult or entity which is able to pay.

Unless the regulator is given sufficient powers to challenge the ways surveillance advertising drives a platform's decision-making, we would expect this business model to continue to incentivise platforms to prioritise behavioural profiling and serving adverts at the expense of children's safety and wellbeing. For example, we find it hard to imagine a situation where the current draft regulations would lead to a platform dropping on safety grounds a functionality which it considered key to surveillance advertising.

3. Surveillance advertising is itself a type of content which is harmful to children.

Despite surveillance advertising being a significant category of content on user-to-user services, and one with a well-documented association with harms, clause 39(2)(f) explicitly exempts all paid-for advertisements for the scope of the draft Bill. We consider this to be an ill-judged exemption, particularly in the case of children.

Surveillance advertising is particularly risky for children because their brains and sense of self are still developing. They are less equipped to understand how behavioural profiling works, and are more vulnerable to being manipulated.

Children's use of the internet should play an important role in their development into well-rounded adults, by enabling them to explore ideas and interests freely - but the ubiquity of surveillance advertising means that their development can be unduly influenced and manipulated.

The volume of surveillance advertising to which children are exposed is significant. A Global Action Plan survey of teenagers revealed that, whilst scrolling through their Instagram feeds on average teens see one ad every 8.1 seconds. This is equivalent to 444 adverts per hour. Based on average online time, this means that a third of 14 year olds could be exposed to 1,332 adverts a day – ten to twenty times as many adverts as children see on TV alone.

In addition, surveillance advertising frequently enables children to be targeted with harmful products, or on the basis of profiling which has identified them to have potentially risky interests. A 2021 study found that it was possible, using Facebook's admanager, to target

children on Facebook aged between 13 and 17 based on such interests as alcohol, smoking and vaping, gambling, extreme weight loss, fast foods and online dating services.

The government will justify clause 39(2)(f) by arguing that a regulatory framework for advertising already exists. We don't think this argument stands up. The current regulatory framework for advertising has proved unfit for surveillance advertising. The growth of social media sites underpinned by a surveillance advertising business model has transformed the quantity and quality of advertising to which children are exposed, and the current regulatory regime is clearly failing to protect children adequately.

4. How the government could tackle surveillance advertising for children

The Online Safety Bill, and the government's broader Online Harms agenda, should recognise the harms and risks associated with surveillance advertising for children, and introduce measures to address these harms. Our recent report explored in detail various options for how this could be done.

1. **Ban all surveillance advertising.** The most straightforward and effective way to protect children from the harms of targeted advertising may be to simply prohibit surveillance advertising practises for all users, regardless of age. Doing so would avoid the complexities of age verification, or of attempting to improve through regulation an intrinsically intrusive and manipulative set of advertising practices. Such a ban could be achieved through banning website or app owners from using users' personal data to sell ad space, and from sharing users' personal information to real time auctions for ad space. Platforms would be forced to switch to other forms of online advertising which don't rely on surveillance of individual users, such as contextual advertising.

2. **Ban surveillance advertising to under-18s.** Enforcement action could be taken against companies failing to take reasonable steps to ensure that they don't serve surveillance adverts to under-18s. Platforms would need to switch surveillance advertising off by default, with only those users that the platform has actively determined are over 18 receiving them. In practice, this would give user-to-user services likely to be accessed by children a choice: either develop sufficiently robust ways of enabling adult users to prove their age in order to opt in to surveillance advertising, or switch to other forms of advertising for all ages. Platforms would be free to develop their own approaches to ensuring only over-18s received surveillance adverts, but would need to satisfy the regulator that their approach was sufficiently robust. The burden would be placed on platforms to protect children from these adverts by default and by design - not on children or their parents/carers to opt out.

Restricting surveillance advertising would not restrict online advertising *per se.* It would likely drive a shift towards more widespread use of "contextual" advertising - adverts placed

on the basis of the content they appear alongside, rather than on the basis of personal information held about the user. There's evidence this form of advertising is a viable alternative for both publishers and advertisers. Contextual advertising removes much of the opacity and huge overheads for adbuyers associated with real-time-bidding systems, alongside mitigating many of the societal problems associated with surveillance advertising.

The government may insist that measures to restrict or regulate surveillance advertising for children are beyond the scope of the Online Safety Bill. We believe that this omission is a mistake, given the Bill's strong focus on protecting children and the clear relationship between surveillance advertising and many of the harms which the Bill seeks to tackle.

It is worth noting that as other jurisdictions develop their own regulatory regimes for social media, they are beginning to accept that surveillance advertising should be within scope. The EU Commission's proposal for the DSA package already includes measures to improve transparency and place some limits on targeting and psychological profiling, and both the European Parliament and the European Data Protection Supervisor (EDPS) have called for further restrictions to be considered up to and including a ban.

If the government insists these issues are outside the Bill's scope, at a minimum it should during the Bill's passage set out what is then its favoured route. Given the Bill will establish Ofcom as the statutory online safety regulator, it must set out how effective coordination between Ofcom, the ICO, the ASA, and the CMA/DMU can best be achieved to address these issues in the future.

Conclusion

The draft Bill is significantly weakened by its failure to address the surveillance advertising business model. A regulator which is unable to challenge the role of this business model in driving a platforms' choices about design and systems, including those with implications for children's safety, will struggle to deliver safe and healthy online spaces. In addition, the blanket exemption for paid-for advertising takes out of scope a huge category of potential harmful content.

We urge your committee to challenge these omissions. If the government proves unwilling to include measures to tackle harms from surveillance advertising within the scope of the Online Safety Bill, they should at least be pressed to set out where such issues may be addressed in the future.

This submission is supported by:

- Global Action Plan
- The Mission and Public Affairs Council of the Church of England
- Global Witness
- New Economics Foundation

- Foxglove Legal
- Fairplay
- 5Rights Foundation
- Andrew Simms, Co-Director, New Weather Institute
- Dr Elly Hanson, Clinical Psychologist
- Avaaz
- Defend Democracy
- Defend Digital Me
- Stop Funding Heat
- The Signals Network

Further information

I-Spy: the billion-dollar business of surveillance advertising to kids is available to read here.

27 September 2021