End Surveillance Advertising to Kids coalition—written evidence (DRG0017)

House of Lords Communications and Digital Committee inquiry into Digital Regulation

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. Surveillance advertising is currently the pre-eminent business model of many of the most popular sites on the internet.

Our recent report,[1] 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 first two questions from your Call for Evidence, "How well coordinated is digital regulation?", and "Do regulators have the powers and capabilities, including expertise, to keep pace with developments?" In our view regulation of surveillance advertising is currently inadequate, insufficiently coordinated, and overseen by regulators who lack the powers, duties, and capacity to tackle harms:

- The self-regulatory regime overseen by the ASA has manifestly failed to prevent a proliferation of unethical and manipulative online ads, based on unethical and manipulative targeting. Its reliance on a mainly reactive and complaints-based approach appears unfit for preventing harms associated with modern surveillance advertising.

- There's a case to be made that the 2018 Data Protection Act should provide a degree of protection for users from intrusive and manipulative uses of data for profiling for targeting adverts, however as yet the ICO has not chosen to interpret or enforce it in this way. We hope that, in the case of children, the Age Appropriate Design Code could mark the beginnings of a robust approach by the ICO. However, we are concerned that the government's apparent intention to relax data protection rules, as set out in *Data: A new direction,* could mean such protections are weakened, even before they begin to be properly enforced.

---

1 https://bit.ly/2RXkUoi

- The draft Online Safety Bill contains an exemption for all advertising content, and so would do nothing to fill current regulatory gaps or challenge the ways in which surveillance advertising incentivises platforms to make decisions about their design, systems, and processes which allow harms to proliferate.

- It is unclear what legislation, if any, will follow the "Online Advertising Consultation" which was promised earlier this year - or how this will generate more progress than the similarly named consultation held less than two years ago. We are concerned that this promised consultation could serve as a piece of long grass, into which concerns about the advertising exemption in the Online Safety Bill can be kicked.

The UK government's July 2021 policy paper, *Digital Regulation: Driving growth and unlocking innovation* proposed as a key principle that "regulatory interventions should address underlying drivers of harm rather than symptoms". We strongly agree with this principle, but do not currently see it being applied to regulation of surveillance advertising.

This submission explains why the current failure to address surveillance advertising in the Online Safety Bill, or anywhere else in the digital regulation or online safety agenda, goes against the government's stated intention of tackling "underlying drivers of harm". We set out how improvements in the safety of social media platform's design, systems and processes is essential if the online harms agenda is to succeed, for two main reasons:

A. **Surveillance advertising is the dominant business model which drives most 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.

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

This submission is therefore quite critical of the current regulatory regime. We do however, recognise that it is a work in progress, and that there have been recent welcome steps in the right direction, such as the Age Appropriate Design Code. The specific criticisms we outline below are offered alongside support for the principle of improved regulation of digital platforms, and an end to a failed reliance on self-policing.

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

Surveillance advertising is the pre-eminent business model of the contemporary internet, including all the most popular social media platforms used by 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. 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 5-Rights 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."*

3. Current regulation of the surveillance advertising business model and its associated systems, processes, and functionalities, is manifestly inadequate

Current regulation, under the ASA and the ICO, has allowed a proliferation of the kinds of harms mentioned above, and so is clearly inadequate.

We welcome the Age Appropriate Design Code as a step in the right direction, in particular the principles that privacy settings for children should be "high" by default, and profiling usually turned off by default. However, whilst this Code does appear to be driving some changes to platforms' designs (proving that regulations produced in the UK *can* have an impact on the behaviour of these global platforms), we are concerned that these changes will not be sufficient.

For example, whilst Facebook has announced a reduction in the targeting options it offers to advertisers to reach under-18s, it appears Facebook will continue to harvest children's data, and use this data in their machine learning enabled 'Delivery System' to optimise targeting in children's feeds. So while Facebook says it will no longer allow advertisers to selectively target teenagers, it appears Facebook itself continues to target teens, only now with the power of AI. In other words, it appears that the Age Appropriate Design Code may be forcing Facebook to make some tweaks to how it implements its surveillance

advertising-based business model for under-18 users, but not fundamentally move away from it.

We are concerned that the government's plans to relax current data protection rules, as set out in September 2021's *Data: a new direction*, could mean that existing protections are watered down just as the ICO, via the Age Appropriate Design Code, is beginning to enforce them more robustly. In particular we are concerned that a relaxation of the "purpose limitation" principles in the GDPR, which (if properly enforced) should limit platforms' processing of a user's data for purposes other than those for which it was originally shared, could further weaken regulation of behavioural profiling for ad targeting and recommender algorithms.

The draft Online Safety Bill could be an opportunity to build on the start made by the Age Appropriate Design Code, however the current draft misses this opportunity. It 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 Online Safety 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 (section 39(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 Ofcom, as 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.

4. Surveillance advertising is a category of online content which is frequently harmful to children

The volume of surveillance advertising to which children are exposed is significant. A Global Action Plan survey[2] of teenagers revealed that, whilst scrolling through their Instagram feeds, on average teens see one ad every 8.1

[2] https://www.globalactionplan.org.uk/files/kids_for_sale.pdf

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.

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.

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.

Despite Facebook's recent announcement that it will remove advertisers' ability to target teens in this way, concerns remain that Facebook's own algorithm will continue to 'optimise' ads for teen users on Facebook & Instagram. As the Facebook whistleblower, Frances Haugen, testified to congress:

> *"I'm very suspicious that personalised ads are still not being delivered to teenagers on Instagram, because the algorithms learn correlations. They learn interactions where your party ad may still go to kids interested in partying, because Facebook almost certainly has a ranking model in the background that says this person wants more party-related content".*[3]

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) of the draft Online Safety Bill 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.

5. Current advertising content regulation, developed for older forms of advertising, is unsuitable for regulation of surveillance advertising

The government will justify plans to exempt paid-for advertisements from the draft Online Safety Bill by arguing that the ASA already oversees a regulatory framework to ensure advertising is not misleading, harmful, or offensive. Whilst we agree that "double regulation" should be avoided, we don't think this argument stands up because 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

[3] Rev Transcripts 2021 'Facebook Whistleblower Frances Haugen Testifies on Children & Social Media Use: Full Senate Hearing Transcript' https://www.rev.com/blog/transcripts/facebook-whistleblower-frances-haugen-testifies-on-children-social-media-use-full-senate-hearing-transcript

quantity and quality of advertising to which children are exposed, and the current regulatory regime is clearly failing to protect children adequately.

Researchers at Oxford University have suggested a fundamental reason[4] why pre-existing regulatory frameworks have proved unable to protect children from harmful content delivered by surveillance advertising. The UK's existing system of regulation for advertising relies on complaints-based mechanisms by which irresponsible, unethical or dangerous advertising can be initially challenged by concerned third parties. This is ineffective for surveillance advertising because of a phenomenon they termed "epistemic fragmentation". Those making complaints are likely to be informed, concerned, motivated citizens who "are not themselves vulnerable, but are aware of those more vulnerable to harm." With surveillance advertising this doesn't work because "consumer's 'personal context' is hidden from others, meaning nobody knows exactly what others see and cannot raise a complaint on their behalf".

In 2015 a London Underground advert by a company called Protein World, depicting a very slender model and asking commuters if they were "beach body ready", prompted hundreds of complaints to TfL and the ASA, and a change.org petition targeting the company. The advert was withdrawn, an ASA complaint upheld, and TfL introduced new guidelines around the depiction of female bodies in tube adverts. A similar "body-shaming" advert on social media, micro-targeted to teenagers profiled as anxious about their weight, is much less likely to face the same level of challenge. A vulnerable teenager with body image issues is relatively unlikely to raise a complaint. Those citizens more likely to challenge it (e.g. a parent, a teacher, or a Child and Adolescent Mental Health practitioner) most likely won't see it, and even if they did wouldn't see who else is being targeted. The governance mechanisms which have, albeit imperfectly, protected children from other forms of harmful advertising simply do not, and cannot, work effectively for surveillance advertising.

It's perhaps not surprising, given these fundamental obstacles to the ASA model being applied to surveillance advertising, that in 2020 only 2,682, or 11.3%, of the ASA's 23,775 cases concerned online, paid-for, advertising. This is despite digital advertising accounting for over 70%, or £17 billion, of UK ad spend over the same period. It seems hard to believe that this huge discrepancy is because misleading, harmful, or offensive adverts are so much rarer an occurrence online.

As we explain below, the simplest and most effective way to use the Online Safety Bill to address the inability of current advertising regulation to cope with surveillance advertising, would be for the Online Safety Bill to prohibit surveillance advertising. This would mean digital platforms would be required to instead develop forms of advertising, such as contextual advertising, which the ASA regime is much better equipped to regulate.

[4] https://www.nature.com/articles/s42256-021-00358-3.epdf

6. 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. It would relieve the ASA of the task of regulating a form of advertising which, as we explained above, it is ill-equipped to cope with. 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. It reduces the level of "epistemic fragmentation" which has rendered the ASA's complaint-based mechanisms so ineffective against surveillance ads, so would mean that existing regulatory frameworks were immediately less ill-equipped to regulate digital advertising.

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.

We believe the draft Online Safety Bill should be amended in the same direction. If the government insists these issues are outside the Bill's scope, at a minimum parliamentarians should insist the government sets out where and how regulatory gaps and flaws such as those mentioned here will be filled. 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

Given that selling surveillance ads is the pre-eminent business model of many of the most-visited websites and most used apps in the UK, and that such adverts are a major category of content, the inadequacy of its current regulation demonstrates that there is more to do before the UK has a world-class approach to digital regulation.

Part of the answer undoubtedly lies in improved coordination between the various regulators involved, and improved enforcement of existing rules. The Age Appropriate Design Code demonstrates the potential of improved coordination and enforcement to change platform behaviour. However on its own this is unlikely to address in full the impact of the surveillance advertising business model as an underlying driver of harm, particularly to children.

We would suggest that the simplest and most straightforward regulatory intervention would be for the Online Safety Bill to simply ban surveillance advertising. This would eliminate a major driver of harms, eliminate a form of data processing which the ICO has struggled to get to grips with, and remove a type of advertising which the ASA has struggled to supervise. 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[5]
- Foxglove Legal[6]
- Global Witness[7]

[5] https://www.globalactionplan.org.uk/stak
[6] https://www.foxglove.org.uk/
[7] https://www.globalwitness.org/en/campaigns/digital-threats/

- Privacy International[8]
- Avaaz[9]
- Defend Democracy[10]
- Stop Funding Heat[11]
- Dr Elly Hanson, Clinical Psychologist
- Fairplay[12]

Further information

I-Spy: the billion-dollar business of surveillance advertising to kids[13]

Please see the *End Surveillance Advertising to Kids* campaign website[14] for more.

October 2021

8 https://www.privacyinternational.org/
9 https://secure.avaaz.org/campaign/en/disinfo_hub/?fp
10 https://defenddemocracy.eu/
11 https://stopfundingheat.info/
12 https://fairplayforkids.org/
13 https://bit.ly/2RXkUoi
14 https://www.globalactionplan.org.uk/post-consumerism/end-surveillance-advertising-to-kids