House of Lords Select Committee on Communications
The Internet: To Regulate or Not To Regulate?

IAB UK submission

Background

1. IAB UK is the trade association for digital advertising, representing over 1,200 of the UK's leading brands, media owners, technology providers and agencies. Our purpose is to build a sustainable future for digital advertising, a market that was worth £11.55bn in the UK in 2017.

2. The IAB is actively engaged in working towards the optimal policy and regulatory environment for the digital advertising market to continue to thrive. We also seek to promote good practice to ensure a responsible medium.

3. Our submission focuses on two main aspects of the terms of reference as they relate to digital advertising: legal liability, and the use of personal data.

Regulation of digital advertising

4. As the Committee's call for evidence recognises, existing regulation and self-regulation applies online. There are a number of key pieces of legislation that apply to digital advertising, including in relation to data and privacy, consumer protection, and 'information society services'. As the call for evidence notes, digital advertising is also regulated by the Advertising Standards Authority (ASA) which enforces the UK Code UK Code of Non-broadcast Advertising, Sales Promotion and Direct Marketing (CAP Code). The CAP Code reflects the provisions of the Consumer Protection from Unfair Trading Regulations 2008 which prohibit certain unfair and misleading practices, and requires that all advertising – including online – is obviously identifiable as such. There is also self-regulation in the digital advertising sector in relation to providing people with transparency and control over online behavioural advertising (see Appendix 1).

5. The industry continues to develop its self-regulatory initiatives to respond to challenges. For example, in March this year, a new joint initiative was announced between JICWEBS[1] and the U.S.-based Trustworthy Accountability Group (TAG) . In the area of ad fraud, TAG has set up the Certified Against Fraud Program, involving anti-fraud guidelines, and a trust seal which means companies can publicly communicate their commitment to combatting fraudulent non-human traffic in the digital advertising supply chain. JICWEBS and TAG have committed to working together to on transfer learnings between the respective initiatives to improve their effectiveness and create a united and consistent approach across markets to tackle criminal activity and clean up the digital ad supply chain.

6. **We believe that the existing regulatory framework for digital advertising is robust, proportionate and effective. This is complemented by industry-led self-regulation, which has expanded over time in response to new issues and enjoys wide support within the ecosystem. We believe this approach is appropriate to ensure that the digital advertising industry operates responsibly and can have a sustainable future.**

[1] The joint industry committee that oversees self-regulatory initiatives including developing good practice principles and certification in relation to brand safety, ad fraud and viewability. See https://jicwebs.org/.

IAB UK
67-68 Long Acre
London
WC2E 9JD

0207 050 6969
info@iabuk.com
www.iabuk.com

Registered in England number 03650406

Digital Charter

7. We share the Government's ambition to make the UK the best and safest place for online advertising and the digital advertising sector has worked with others in the advertising industry, under the auspices of the Advertising Association, to identify areas where the Government could support industry efforts to tackle some of the issues that threaten to undermine consumer and business trust in digital advertising.[2] These can be summarised as:

- Ad fraud: ensure appropriate law enforcement action is taken against criminals who abuse the digital advertising ecosystem for financial gain
- Ad misplacement: support existing initiatives and encourage compliance with industry standards and good practice (e.g. the JICWEBS DTSG Brand Safety Good Practice Principles)
- Ad blocking: maintain equivalence with the EU 'net neutrality'3 rules post-Brexit; recognise the value of the ad-funded business model, which supports the development and provision of digital services, content, and apps; support publisher efforts and wider industry work to improve the ad-funded experience online through the Coalition for Better Ads
- Data privacy: prioritise discussions on data-sharing in Brexit negotiations and allocate resource to ePrivacy Regulation negotiations (see paragraph 28 below).

Legal liability of online platforms

8. Digital advertising operates within a complex ecosystem and relies upon the collaboration of multiple players including advertisers, ad buyers, demand aggregators, supply aggregators, technology providers, creative agencies, measurement and assurance providers, and media owners.

9. A range of legal and self-regulatory frameworks, as well as technical standards, serve to support this ecosystem. Among the foundational legal frameworks is the regime which governs the assignment of rights and responsibilities within the digital ecosystem. This is enshrined in Articles 12-15 of the eCommerce Directive, and is expressed as limitations to liability for online intermediaries, but in practice balances rights and responsibilities between a far broader range of players in complex digital environments. It is important that the Committee appreciates the broader application of this legal framework and its particular relevance to digital advertising.

10. This legal framework has characteristics which make it adaptable to a range of digital environments, including advertising. By engaging specific activities, rather than a particular business model or technology platform, it is technology neutral and applies in a targeted way. This means that companies with complex business models – where they may be an intermediary for some activities but not for others – can confidently apply the principles to different activities they perform and have legal clarity. For example, a company that has a news publishing business and also has an ad platform business would be legally responsible (in this specific example) as a publisher for its editorial content but could also be an intermediary (with differentiated liabilities) for certain activities relating to the operation of its ad platform.

---

[2] See https://www.adassoc.org.uk/wp-content/uploads/2017/12/AA_Digital_Charter_2017_SinglePages_15.11.17.pdf

[3] Net neutrality is an important principle that protects against network-level ad blocking (e.g. at mobile network operator level) and existing guidelines, based on the EU 'Universal Service Directive', state that all internet users should have equal access to content and advertising online to ensure telecoms operators cannot block content.

11. Crucially, the principles of this framework are woven into a range of industry initiatives and self-regulation including the UK CAP Code on non-broadcast advertising. The Code assigns primary responsibility for advertising content and decisions about targeting to the advertiser, whilst engaging media owners, for example, to help enforce ASA adjudications and terminate non-compliant campaigns where an advertiser fails to act, or engaging advertising intermediaries to surface evidence to aid investigations into breaches of the Code. Similarly, the EDAA principles on behavioural advertising (see Appendix 1) commit advertisers to defined obligations around targeting decisions whilst also place other obligations on advertising intermediaries that reflect their role and position in the ecosystem.

12. In the context of editorial control, tensions can arise between the liability principles that apply to 'information society services' (e.g. under Article 14 of the e-Commerce Directive) and questions around how illegal content online should be managed or moderated. Actions taken in good faith by service providers could potentially be aided by having an equivalent defence to that in Section 230 of the U.S. 1996 Communications Decency Act that affords a 'Good Samaritan' protection for blocking and screening of offensive material. The Committee could explore the feasibility and benefits and drawbacks of this approach.

13. The principles of the underlying legal framework set out in the e-Commerce Directive provide the foundations on which self-regulatory initiatives are built and give confidence to the parties involved to collaborate to resolve challenges which arise in digital advertising. These are not legal issues which could easily be addressed contractually in such a complex commercial and technical environment. Shifting away from the activity-based approach, or modifying this regime for some types of technologies and/or business models but not others, would have a disruptive and unpredictable impact on the digital ecosystem and the ability of its component operators to collaborate. **The IAB would urge the Committee to proceed with a high degree of caution on this issue.**

Regulation of the use of personal data in digital advertising

14. The use of data and the protection of privacy in digital advertising is currently governed by the Data Protection Act 1998 (shortly to be superseded by the General Data Protection Regulation (GDPR)), and the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2003 (PECR) (which derive from European Directive 2002/58/EC, also known as the 'ePrivacy Directive'). Both are enforced by the Information Commissioner's Office in the UK.

Data protection law

15. The Data Protection Act 1998 governs the collection and processing of data and will shortly be superseded by the General Data Protection Regulation (GDPR), which comes into force from 25 May 2018 in all EU member states, including the UK.

16. The GDPR updates the existing EU data protection framework and aims to give individuals more transparency about and control over whether and how their personal information is used. It regulates the use of all personal data in digital advertising (information such as an online identifier – e.g. an IP address – can be 'personal data'). Some of the key provisions introduced by the GDPR, and that are relevant to digital advertising, are:

- Organisations will require a legal basis to process personal data. There are six legal bases available, but those most commonly used in the digital advertising sector are 'consent' and 'legitimate interests'.
- The GDPR strengthens the conditions for consent. Consent will need to meet very high standards (e.g. it cannot be bundled with Ts&Cs) to be relied on as a legal basis for processing personal data. The user will also need to give consent 'unambiguously' with an affirmative action. Processing 'sensitive' personal data (e.g. racial or ethnic origin / sexual orientation) requires the user's explicit consent.
- In all cases, evidence that consent has been obtained will have to be recorded, meaning organisations that have no direct relationship with the user will have to find a way to obtain consent indirectly.
- The introduction of increased sanctions: organisations can be fined up to €20m or 4% of annual turnover (whichever is greater) if they breach the law.
- The GDPR also introduces special protection for children's personal information: if an organisation collects information about a child and is relying on consent to process it lawfully then it will need a parent's/guardian's explicit consent where the child is under a specified age (expected to be 13, in the UK).

17. The GDPR applies to both 'data controllers' (i.e. an organisation that decides how and why personal data is processed) and – for the first time – 'data processors' (i.e. an organisation that specifically acts on a controller's behalf). Businesses involved in the processing of personal data for digital advertising purposes will be classified as either a data controller or a data processor under the GDPR.

18. Obligations for data controllers include transparency – the GDPR extends the amount of information organisations must provide to individuals about how they use personal data (e.g. an organisation's legal basis for processing personal data, data retention periods, the use of third party data etc.) – and accountability. The GDPR also requires that information given to people about the processing of their personal data is easy to understand and written in plain language.

19. IAB UK has produced a briefing[4] on GDPR and digital advertising, which is enclosed with this submission. We draw the Committee's attention in particular to the following sections, which provide more detail about what the GDPR means for digital advertising, the additional responsibilities it creates for data controllers and processors, and the extensive rights that it confers on individuals.

- Section 4 – Legal Bases
- Section 5 – Obligations for Data Controllers and Data Processors
- Section 7 – Individual Rights & Control

20. In addition, the IAB's GDPR preparation checklist[5] explains in detail the key aspects of the GDPR as they relate to businesses in the digital advertising sector.

[4] https://www.iabuk.com/policy/eu-general-data-protection-regulation-gdpr-briefing-digital-advertising-industry
[5] https://www.iabuk.com/policy/iab-uk-gdpr-checklist

21. **The provisions in the GDPR mean that individuals will have more information about and control over whether and how their data is used.**

Cookies and other similar technologies

22. PECR sets out specific rules on rules on the storing of information or gaining access to information already stored on a device (whether personal data or not), i.e. cookies and similar technologies (in this submission we use 'cookies' to mean either or both of these). Cookies are widely used in digital advertising, for example to help personalise advertising and measure its outcome.

23. PECR requires that users are told if a site, app, etc. wishes to drop a cookie or access a stored cookie on their device, and given a clear explanation of what the cookies do and why (this is usually managed via a 'cookie banner' that you see when you visit a website). Specifically, the site must get the user's consent to store or access a cookie on their device.[6] The GDPR does not supersede PECR and it remains in force in the UK as well as other EU countries that have implemented it. However, the GDPR changes the definition of 'consent' as it applies to PECR and the use and access of cookies.

24. In practice, this means that – from 25 May 2018 – consent has to be sought from the individual before a cookie is set or accessed. That consent, under GDPR, has to be freely given, specific, informed and unambiguous and requires a positive action from the individual to be valid.

25. **Taken together, the provisions of the GDPR and PECR mean that individuals will know when and how their personal data is being or could be used for digital advertising purposes, whether by a first party (e.g. the site or platform that they are accessing) or a third party (e.g. an advertising technology company) and will have the ability to choose whether and how their data is used (and to change this at any time).**

The effect of Brexit

26. The regulation of the use of personal data is, as outlined in our submission, key to the regulation of digital advertising.

27. The digital advertising ecosystem is a global business and relies on the free flow of data. The free flow of data between the EU and the UK (in both directions) will be crucial. We welcome the inclusion of data flows as one of the top five Brexit issues and the commitment to implementing the GDPR in full and maintaining regulatory alignment.

28. We welcome the Committee's recommendations in its previous report. 'UK advertising in a digital age', that the UK Information Commissioner's Office should retain a place on the European Data Protection Board following the UK's exit from the EU.

29. We also share the Committee's concern, as set out in that report, that Brexit will cause the UK to lose its influence in setting EU rules for data protection which the UK is likely to remain aligned with post-Brexit. This is particularly relevant in relation to the proposed ePrivacy Regulation (ePR), which will review and update the ePrivacy Directive (the basis for PECR) and would apply across all EU member states. The proposed ePrivacy Regulation threatens the future of the data-driven digital economy and could greatly undermine the investments made in GDPR implementation efforts. Even though the UK may have left the EU at the time of its application, UK businesses may in practice

[6] There is an exception for cookies that are essential to provide an online service at someone's request (e.g. to remember what's in their online basket, or to ensure security in online banking).

have to adhere to it to ensure continued provision of services to EU markets. As such the development of the Regulation still needs the full involvement of UK authorities. **This is critically important as the Regulation passes through crucial stages of the negotiations**.[7]

30. In practice, many digital advertising companies operate across EU markets and globally, and a consistent and harmonised regulatory approach is preferable, particularly in terms of issues such as data and privacy. However, these approaches also need to be pragmatic and take a proportionate approach to managing relative risk. **Brexit may present an opportunity to improve on existing or potential new laws, such as the ePrivacy Regulation, and this should be balanced against the risk of developing fragmented or disparate legal frameworks, particularly in the context of the internet, which is by its nature global and without borders.**

[7] https://www.iabuk.net/news/european-parliament-committee-s-approach-on-eprivacy-would-harm-european-media-and-citizens

Appendix 1: EDAA Framework for Online Behavioural Advertising

In addition to legislative requirements and the mandatory self-regulatory system of CAP and the ASA, the digital advertising industry has established self-regulatory frameworks in other specific areas in order to set out accepted standards and good practice for responsible advertising. One such framework covers the use of personal data for online behavioural advertising.

IAB UK acknowledges that the collection and use of consumer data (such as web browsing and other information) could potentially raise issues relating to consumer privacy. In 2011, building on an US initiative and the development of good practice in the UK, EU advertising and media trade bodies published good practice for all EU and EEA markets to enhance transparency and user control for online behavioural advertising (OBA). This framework applies to advertising targeted at any user, including those aged under 18, with specific provision relating to younger children, as described below.

The initiative is based upon seven key principles:

i. Notice: Transparency about data collection and use practices associated with behavioural advertising, providing consumers with clear, prominent and contextual notice through multiple mechanisms, including an icon in or around advertisements linked to further information and control mechanisms.
ii. User choice: Greater consumer control over behavioural advertising. For example, via www.youronlinechoices.eu.
iii. Data security: Appropriate data security and retention of data collected and used for behavioural advertising purposes.
iv. Sensitive segmentation: This principle recognises the need for additional protection for younger children, and requires participating businesses to agree not to create 'interest segments' to specifically target children (12 and under) and on the collection and use of sensitive personal data for behavioural advertising.
v. Education: For consumers and businesses about behavioural advertising and the self-regulatory Framework.
vi. Compliance and enforcement: Mechanisms to ensure the effectiveness of the Framework, including a trading seal to be granted to compliant businesses once independently audited and which demonstrates to other businesses that the holder adheres to the obligations under the Framework.
vii. Review: Regular review of the Framework to ensure it evolves with developing technology and business practices. For example, in 2016 the EDAA extended the existing principles to the mobile environment, so that they apply to ads shown on smartphones and tablets in addition to desktops and laptops.

A copy of the EU industry Framework can be found at: http://edaa.eu/european-principles/. At the heart of this work is a symbol or icon (see below right – often known as the 'AdChoices' icon) that appears in or around the advertisements on sites, as well as on site pages themselves. When a user clicks on the icon he or she will be able to find out more about the information collected and used for this purpose. In 2017, over 170bn icons were delivered by approved providers across Europe,

giving consumers significant opportunities to manage or control their online advertising preferences.[8]

5.6 The icon also links to ways for internet users to manage their interests, such as via privacy dashboards or ad preference managers. It also links to a pan-European website – www.youronlinechoices.eu – with helpful advice, tips to help protect privacy and a control page where you can turn off behavioural advertising. There are on average 1.9 million unique visitors to www.youronlinechoices.eu every month.[9] The UK version of the website is at www.youronlinechoices.eu/uk. Further information on the initiative is available at https://www.iabuk.com/policy/iab-factsheet-may-2014-online-behavioural-advertising.

The EU industry initiative is administered by the European Interactive Digital Advertising Alliance (EDAA) www.edaa.eu. The ASA administers OBA consumer complaints in the UK and in 2013 new rules on OBA were introduced to the CAP Code to ensure businesses provide:

- notice to be provided to web users **in or around the advertisement**;
- choice via an **opt out mechanism** to prevent data from being collected and used for behavioural ad purposes.

These rules are **complementary** to the EU Framework: those businesses complying with the EU Framework will be complying with the CAP Code.

It should be noted that it remains to be seen whether and how this Framework will operate once GDPR comes into effect, as a number of the aspects that it covers (such as notice, choice, and sensitive segmentation) are now covered by the GDPR. [10]

[8] https://www.edaa.eu/ext/edaa_2017.html
[9] ibid.
[10] In response to changes introduced by the GDPR, the Committee of Advertising Practice (CAP) is consulting on changes to the rules related to the collection and use of data for marketing. https://www.asa.org.uk/news/gdpr-consultation-on-the-collection-and-use-of-data-for-marketing.html