

Digital Charter: Advertising Association proposals to Government

November 2017



**ADVERTISING
ASSOCIATION**

Contents

Who are we? — 02

Making the UK the best and safest
place for digital advertising — 04

Advertising Fraud — 06

Advertising Misplacement — 12

Ad Blocking — 18

Data: Privacy & cross-border
data flows — 24

The Advertising Association promotes the role, rights, and responsibilities of all commercial communications for the whole ecosystem including advertisers, media owners, agencies, and ad technology companies.

These proposals, developed by a working group chaired by IAB, represent the advertising industry's collective input to the Government's Digital Charter work programme. Along with the AA and IAB, the following organisations are on the working group: ISBA, the IPA, the NMA, Facebook, Google, Sky, RhythmOne and CAP/BCAP.

We recognise that as part of the Digital Charter work programme the Government will be looking at how it can ensure there is a sustainable business model for high-quality content online. Our members will continue to engage bilaterally with the Government as it explores these issues.

Making the UK the best and safest place for digital advertising

We share the Government's ambition to make the UK the best and safest place for online advertising. We want the country to represent a gold standard in digital for others to admire, follow and emulate and ensure that the UK retains its leading role in e-commerce and digital advertising.

Digital advertising is a vibrant and successful sector delivering brand value and powering a significant proportion of the UK's digital and creative economy. In 2016, digital adspend at £10.3 billion accounted for half of total adspend, and the UK's digital advertising economy is larger than its German and French counterparts combined.

Self-regulation is a crucial element in the UK's leadership in digital advertising. The ASA system covers all digital advertising and marketing and serves as a blueprint for successful advertising regulation in many markets around the world. The industry is committed to maintaining an effective self-regulatory system and is currently in discussions to ensure its sustainable funding.

Summary: four areas to address:

The following four areas have the potential to undermine consumer and business trust in digital advertising:

1. Advertising fraud: where there is a need to ensure appropriate law enforcement action is taken against criminals who abuse the digital advertising ecosystem for financial gain.
2. Advertising misplacement: where there is a need to protect consumers by ensuring that ads do not incentivise the production or dissemination of harmful or extremist content.
3. Ad blocking: where there is an existential threat to online content and businesses, and a consequent need to ensure consumers have a positive experience online whilst safeguarding the ability of online publishers to monetise their content through advertising.
4. Data privacy: where there is a need to ensure that UK citizens enjoy high levels of protection, subject to robust freedom of expression and freedom of information exemptions, whilst also ensuring that data flows freely to and from the UK so that it remains a world-leading centre for delivering innovative digital services.

ADVERTISING FRAUD

What is it?

Ad fraud is the deliberate generation of fraudulent, often non-human traffic (i.e. visits to an online site/page) in an attempt to extract money from the advertising ecosystem. Several types of ad fraud exist but they generally have one or more of the following characteristics¹:

- Illegitimate and non-human traffic (e.g. bots)
- Intentional misrepresentation
- No chance of the ads being seen by a legitimate human audience

Why this is an industry concern:

All parts of the advertising ecosystem can be affected:

- Advertisers are at risk of paying for advertising that reaches no one and therefore returns no value to their brand.
- Legitimate publishers can lose out as the diverted revenue is not being used to support genuine content creators.
- Ad tech suppliers can incur commercial and reputational losses if fraudulent actors take advantage of their systems. This can make them liable for rebates or refunds to advertisers and their agencies.

1. See JICWEBS UK Traffic Taxonomy for Digital Advertising Version 1 (October 2015)

What is the public policy implication?

Those organising and conducting ad fraud may be generating revenue to fund organised crime and terrorism. This is a significant issue for brands and genuine content creators, diverting a significant amount of revenue². It is also a serious policy risk.

Even if only a small percentage of the £10bn digital ad spend is diverted through fraud, this could be very significant. The Government's concern about cybercrime and the potential risk to terrorism makes this, we suggest, a significant priority for the Government to help tackle through the Digital Charter work programme.

2. There is no reliable data available for the cost of ad fraud in the UK. In the U.S., the 2016 ANA/White Ops Bot Fraud study estimated that advertisers lose \$7.2 billion per year globally (of an estimated total \$194.60 billion spend on digital advertising in 2016 (eMarketer)) to bot-generated, non-human traffic (projected losses for 2017 are lower, at \$6.5 billion of a total \$229.25bn).

What the industry is doing:

1. JICWEBS – creating industry standards:

JICWEBS, the Joint Industry Committee for Web Standards in the UK and Ireland, has developed initiatives to promote confidence by certifying to advertisers and media agencies that their digital campaigns are reaching the intended audience and minimizing non-human traffic in web analytics.

To help tackle ad fraud and create a safer, more transparent supply chain, JICWEBS has developed:

- Industry guidance on risk reduction.
- Ad fraud definitions that describe illegitimate, non-human traffic sources. These help ensure that the industry has a common understanding of what constitutes fraud.
- Good practice principles aimed at reducing the risk of exposure to fraud. These cover fraud education and policies, and set correct campaign returns on investment targets (ROIs), ad inventory sources and anti-fraud technology and vendors³.
- Independent certification processes with accompanying ‘seals’ (a) for publishers, agencies and ad tech providers that apply the good practice principles, and (b) for anti-fraud vendors/ad verification suppliers who provide solutions that aim to detect and reduce fraud. 46 companies had signed up by September 2017⁴.

3. <http://www.jicwebs.org/agreed-principles/online-ad-anti-fraud-principles>

4. <https://www.jicwebs.org/agreed-principles/latest-news/201-brand-safety-and-fraud-update>

2. Trans-Atlantic industry initiative:

In March 2017, a new joint initiative was announced between JICWEBS and the US based Trustworthy Accountability Group (TAG)⁵. TAG has set up the Certified Against Fraud Program, involving anti-fraud guidelines and a trust seal. This means that companies can publicly communicate their commitment to combatting fraudulent non-human traffic in the digital advertising supply chain.

JICWEBS and TAG are focused on transferring 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.

3. Measures to counter 'domain spoofing':

Separately, the IAB Tech Lab – an independent research and development consortium that develops global technical standards for the digital advertising industry – recently published the ads.txt initiative. This project is part of a broader effort to reduce the ability to profit from 'intentionally misrepresenting inventory' (known as 'domain spoofing'). It provides a simple solution for publishers to declare who is authorised to sell their advertising inventory.

5. <https://iabuk.net/about/press/archive/tag-and-jicwebs-partner-to-clean-up-digital-advertising-supply-chain>

How can the Government help?

Tackling organised ad fraud should be an important priority in the context of the Government's objective of making the UK a beacon in online standards.

Although ad fraud is a global issue, there is an important role for the UK in taking direct action and in giving leadership by supporting a drive towards international enforcement mechanisms.

We propose that law enforcers and the industry could work together, using the industry's existing fraud detection and prevention mechanisms, to help tackle 'malvertising' and other forms of ad fraud and to understand persistent and organised actors and their links to other crime.

The Government could provide a mechanism for the ad ecosystem to engage with law enforcement agencies where industry sanctions have not been sufficient to deter illegitimate actors. A range of enforcement tactics could be explored, similar to those that have been adopted by PIPCU in the fight against IP infringement online.

In summary, Government could:

1. Engage with industry initiatives such as JICWEBS and TAG to support the continued development of industry solutions to address ad fraud in the digital ecosystem.
2. Work with industry better to assess the scale of ad fraud in the UK.
3. Allocate police resource to build understanding and expertise in criminal ad fraud through the National Cyber Crime Unit.

ADVERTISING MISPLACEMENT

What is it?

This is where legitimate advertising is inadvertently placed next to content that is unsuitable for the brand because it is inappropriate, harmful, or illegal. The automated way in which online advertising is bought, which involves a complex supply chain, means that ads could potentially be placed on any number of sites that a person may visit and there is a risk of ads being misplaced.

Why this is an industry concern:

Advertisers, agencies, and ad networks aim to place advertising to reach specific target audiences and to avoid inappropriate online environments. This is commercially important and there is significant investment in mechanisms to prevent misplacement.

Buyers – advertisers, and the agencies buying on their behalf – need transparency in order to define clear policies for where they wish their ads to appear or not appear, and make informed decisions on a campaign-by-campaign basis. Where transparency cannot be provided, there is a risk of advertising being placed next to unsuitable content, some of which may be harmful and/or illegal (e.g. terror-or hate-related content, IP-infringing sites) and some of which may not be illegal but at odds with a brand's policy (e.g. pornography). This has direct reputational cost for the brand as well as all the companies that have played a role in delivering the advertisement.

What is the public policy implication?

The Government has made it a priority to make the UK's online environment as safe as possible, notably for vulnerable consumers. It is important that online ads are being placed responsibly and are not inadvertently monetising illegal content online.

Legitimate advertising revenue may be funding illegal activity and be seen to be 'endorsing' such activity. The link to de-monetising terrorist content makes this particularly important for the Government's wider anti-radicalisation strategy.

What the industry is doing:

1. The industry has developed a cross-industry self-regulatory initiative, the Display Trading Standards Group (DTSG) that is governed by JICWEBS. The DTSG has developed tools to provide transparency and enable buyers actively to manage campaigns and minimise the risk of ad misplacement.
2. The DTSG has published good practice principles for all business models involved in buying, selling and facilitating digital display advertising. There are currently over 60 signatories, covering a significant proportion of the market. To minimise the risk of advertising funding IP-infringing content, for example, the industry has worked with the City of London Police's Intellectual Property Crime Unit (IPPCU) to develop and implement the 'Infringing Website List' (IWL)⁶ that functions in effect as a 'blacklist' of sites that the Police have verified to be infringing copyright. This list enables the industry then to disrupt the ad revenue such sites receive⁷. The DTSG provides a framework for the IWL to be used by the industry.
3. Platforms that host user-generated content such as Google (YouTube) and Facebook have put in place measures to be able better to identify, take down (where appropriate) and/or restrict the monetisation of illegal content such as terror-related content.

6. <https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/Pages/Operation-creative.aspx>

7. The IWL works as an 'inappropriate schedule' and allows companies to exclude known illegal sites from their ad buying, selling, or trading.

4. ISBA is holding discussions on brand safety guidelines with its members, as well as with the Cabinet Office (representing the Government as a major advertiser). These guidelines aim to give guidance to companies on questions to ask their agency, and a series of tips and tools that brands can use to help protect their online reputation.
5. Tightening up procedures and guidance has been a number one issue for the industry bodies and companies in recent months, in order to minimise – if not wholly eliminate – the problem. The industry is exploring how to build on the DTSG framework, including through the partnership between JICWEBS and TAG.

How can the Government help?

1. Develop an information-sharing mechanism with industry to ensure that Government is aware of continuing industry efforts and discussions to minimise advertising misplacement, both domestically and globally.
2. Support the continued development of the best self-regulatory solutions to managing ad misplacement by all parties in the advertising ecosystem, for example, the Brand Safety Principles published by DTSG (the Display Trading Standards Group), which is the preferred mechanism of the advertisers represented by ISBA, the agencies represented by the IPA, the advertising technology companies represented by the IAB and the Association of Online Publishers.
3. Work at the international level to encourage other key markets to strengthen measures to address ad misplacement, notably on foreign language content sites which may be accessed by UK citizens.

AD BLOCKING

What is it?

Ad blocking usually involves people downloading software ('ad blockers') onto their computers or mobile devices to prevent ads from appearing when they are online. People choose to block ads for a variety of reasons:

- because they do not like the advertising (e.g. because it is annoying or interferes with what they are trying to do);
- because they want to optimise the speed and efficiency of their online activity;
- or because they want to minimise the usage of their data allowance.

At present, most ad-blocking tools are relatively blunt in nature. They generally block all display advertising on all sites, unless sites are manually whitelisted by ad blocking operators or individual users. Some operators (e.g. Ad Block Plus) allow certain types of 'acceptable ads' to be delivered, though they levy fees on the biggest advertising operators to serve ads through this system.

Why this is an industry concern:

Ad blocking is disrupting the digital ecosystem. Disruption in and of itself is not necessarily a bad thing, and the industry recognises that the overall digital ad experience needed improving. However, the current deployment of blunt ad blockers is having a particularly negative impact on publishers, undermining their ability to monetise their content through advertising.

Longer-term, if publishers and content-creators are forced to limit access or charge (or charge more) for access to their content, this restricts their potential audience to people who are able or willing to pay for access, and may mean that some publishers' business models are no longer sustainable.

What is the public policy implication?

Advertising is the primary tool to monetise content online and is therefore essential to a sustainable digital advertising industry, a free and open web and viable ad-funded business models (e.g. news).

Ad-blocking threatens these business models and the value exchange of content and services paid for by advertising.

Ad blocking levels in the UK have stabilised but remain a concern⁸. It is important to ensure that, wherever possible, content can be free at the point of consumption to ensure access to a plural media for all elements of society.

8. <https://www.iabuk.net/about/press/archive/ad-blocking-levels-have-stabilised>

What the industry is doing:

1. The Coalition for Better Ads (CBA) – a global consortium of brands, advertising technology companies, publishers, and trade bodies – is the industry’s collective response, focused on improving ad experiences online.
2. Under the ‘DEAL’ approach⁹, publishers have adopted a number of tactics to address ad-blocking and persuade people not to use ad blockers (e.g. identifying when a visitor to their site is using an ad-blocker and restricting their access to free content; explaining the advertising value exchange; implementing paywalls and offering ad-free or low-ad subscriptions). Some have also used technical solutions to prevent ads on their sites being blocked.
3. The industry has adopted the ‘LEAN’ principles¹⁰ designed to improve the online ad experience.
4. The CBA has published initial ‘Better Ads Standards’, based on consumer research. These identify 12 ‘bad’ ad formats that should be avoided. The aim is for the industry to stop paying for, producing, or hosting negative ad formats (e.g. pop up ads) that lead people to block ads. Implementing these standards is actively encouraged by CBA members, including participating trade bodies, which cover a large proportion of the overall digital advertising market.

9. DEAL is the IAB’s recommended approach for publishers to connect with ad blocking consumers through a step-by-step process: Detect ad blocking, in order to initiate a conversation | Explain the value exchange that advertising enables | Ask for changed behaviour in order to maintain an equitable exchange | Lift restrictions or Limit access in response to consumer choice.

Read more at <https://iabuk.net/about/press/archive/iab-releases-adblocking-primer-that-recommends-a-new-deal-between-publishers-and#PotgOlr5QGpOxIGU.99>

10. LEAN: Light, Encrypted, Ad Choice Supported, Non-Invasive Ads

How can the Government help?

Whilst the industry's approach to improving the online advertising experience is based on consumer evidence, it remains unclear whether this will lead to positive results in practice. A continuing technological back and forth between ad blockers and publishers is possible and there are limited competition law and other legal remedies for publishers whose business model is undermined by ad blocking. The Government could support the digital advertising industry in its efforts to tackle ad blocking:

1. Maintain equivalence, when the UK exits the EU, with EU 'net neutrality' rules that require internet service providers to "treat all traffic equally" as it is directed over their networks. 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.
2. Recognise publicly the value of the ad-funded business model which supports the development and provision of digital services, content, and apps.
3. Support publisher efforts to clarify legal avenues to challenge the lawfulness of disrupting legitimate business models through non-user led ad blocking mechanisms.
4. Support industry efforts to improve the user experience through the Coalition for Better Ads.

DATA: PRIVACY & CROSS-BORDER DATA FLOWS

What is it?

In the context of digital advertising, data privacy means balancing individuals' right to privacy with their desire for high-quality digital services and content, which are both free and tailored to people's preferences and interests. Data enables content and advertising to be tailored for, and targeted to, specific audiences.

Cross-border data flows and a practical, proportionate data protection regime are pre-requisites to the effective functioning of digital advertising businesses and to the UK's attractiveness as a place to innovate and operate digital businesses.

Why this is an industry concern:

1. The EU's General Data Protection Regulation (GDPR) comes into force in May 2018 and the industry is preparing for implementation. This is complicated by the lack of guidance from European Regulators on key issues such as consent.
2. Additionally, 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 have to adhere to it to ensure continued provision of services to EU markets. The development of the Regulation still needs the full involvement of UK authorities.

3. The advertising and media ecosystem needs scale in order to be sustainable in the long term. Services need to continue to be provided seamlessly across multiple markets in the future. The free flow of data between the EU and the UK after the UK exits the EU is crucial to this long-term sustainability.
4. Getting the Data Protection Bill and other detailed implementation legislation correct is important, not just for the digital advertising sector but given the wider implications (e.g. the freedom of expression exemptions which are of key importance to news media).

What is the public policy implication?

Data has become key to the UK's economy and powers today's digital media and services. It is crucial to effective advertising and marketing communications as well as the continued success and sustainability of the wider digital economy.

What the industry is doing:

Due to the sensitive nature of processing personal data, and the associated reputational cost and financial sanctions for errors, the advertising ecosystem is investing heavily in ensuring that data privacy is at the core of its activities. Cross-industry work is taking place to ensure that there is a consistent approach to GDPR implementation and that the UK will be able to demonstrate best practice standards of compliance.

How can the Government help?

1. Encourage clarity from the ICO on forthcoming GDPR guidance on key issues like consent.
2. Prioritise UK-EU and UK-U.S. data sharing agreements as part of Brexit considerations.
3. Work with industry to develop common thinking on future compliance issues as a result of opinions issued by the European Data Protection Board.
4. Invest sufficient Government resources into advocating for a pragmatic approach to the proposed ePrivacy Regulation.
5. Encourage ICO support for voluntary industry approaches in the UK, at European and at international level.
6. Ensure that the Data Protection Bill and other implementing legislation implements comprehensive GDPR exemptions for freedom of expression and information and other derogations including those vital to free flow of data across borders.

The Advertising Association

Promoting the role, rights and responsibilities of advertising

The Advertising Association promotes the role, rights and responsibilities of advertising and its impact on individuals, the economy and society. We are the only organisation that brings together agencies, brands and media to combine strengths and seek consensus on the issues that affect them. Through wide-reaching engagement and evidence-based debate we aim to build trust and maximise the values of advertising for all concerned.

7th Floor North
Artillery House
11-19 Artillery Row
London SW1P 1RT

+44 (0) 20 7340 1100
aa@adassoc.org.uk
adassoc.org.uk

For further information, contact:
Sue Eustace, Director of Public Affairs:
sue.eustace@adassoc.org.uk



**ADVERTISING
ASSOCIATION**