Internet Advertising Bureau UK

Future Trends Working Group

Future Trends Volume 11:
Future Threats

Contents

Introduction

Tim Elkington, Chief Strategy Officer, IAB UK

Having written about potentially exciting future developments in the last ten papers produced by the Future Trends Council we felt it was about time to take a different approach and look at potential threats to the future, so welcome to Future Trends 11 – Threats to the Future.

Dan Calladine from Dentsu Aegis wonders if the possibility of paying to access content free from advertising online could damage existing digital business models? With more businesses making money without the need for advertising could the established online media business model be under threat? Dan looks at the likelihood of users changing habits and paying to access content and also the changing nature of digital ads which could make advertising less intrusive to answer these questions.

Tamara Jacobs of Blinkx Media takes a different angle and considers business opportunities that might arise because of future threats. For example we might produce more online data than we're capable of storing in 2015 and this is likely to spark huge amounts of creativity in the storage sector. Couple this with drones and their emerging uses and the future for new businesses in a changing landscape looks exciting.

Juliette Gilligan from Adludio concentrates on Ad Fraud as a threat to the future. Juliette includes action plans for buyers and sellers to mitigate this threat. She also looks at likely developments, including a Cost Per Human (CPH) metric and concludes that tackling fraud will ultimately benefit advertiser as their budgets will work harder and ROI will increase.

Finally Alison Sprague of GEG Europe argues that the future is bright, but looks at regulation as a possible obstacle to future digital advertising growth and considers the recent experiences of Oreo and Groupon in the regulatory area. Alison notes that current industry self-regulation works well in the digital space whilst also looking at the challenges ahead such as content marketing and the need to separate editorial and advertising.

Threats to Advertising – Paying to go ad-free

Dan Calladine, Aegis Dentsu

One of the possible threats of advertising in the coming years is the nascent trend to pay to avoid ads.

Newspapers often with both a payment (cover price) and advertising, giving two revenue sources. TV and radio have historically been ad-funded since it used to be hard to restrict people from accessing a broadcast. Online media has traditionally been ad funded, since while it was possible to block access, publishers found that restricting access (or insisting people log in) meant far less traffic and less influence. (When I was growing up a local cinema used to use the fact that it showed no ads before the film as a USP; it now shows ads)

There's now a feeling that this could be changing, however.

Netflix makes a point of having no ads, making payment to get uninterrupted viewing a major part of its proposition.

Spotify has a free, ad-funded version, and a paid, ad-free version. Consistently about 25% of the users (currently 12.5m out of 50m) pay to be able to stream music with no intrusive ads between songs.

Google is also proposing this with its new Music Key service through YouTube – again pay to get music on YouTube with no ads between the songs.

Google is also experimenting with something called Contributor by Google which will provide an alternative way to fund sites.

Signed up users (it's currently a closed test) pay $1 - $3 a month to be part of the programme. Google measures how often you visit the participating sites, and then at the end of the month divides the money based on how often you visited the different sites. It's very neat, and presumably uses Google's tracking technology and advertising network for the measurement and distribution of the funds to the different sites.

(A similar system, called Flattr has existed since 2010, but without Google's scale and influence)

It's going to be fascinating to see how this works. If it works well then advertisers could find it harder to advertise to audiences online, but there are some potential problems.

It won't be for everyone. Only the comparatively rich can realistically afford to pay to avoid ads. The advertising model has existed for so long because it offers people free access to content. Over 3 billion people are now online – it would be surprising if over 1% (30m) would be willing to sign up to something like this. (Music is different – ads are interruptive and more damage increasingly damage the experience).

What is an ad? Banners are clearly identified as ads, but what about Buzzfeed's (and others') native ads and promoted posts? What about PR? What about tweets and Facebook posts from brands that you follow? Is Google going to decide this? What will Google do with its very valuable list of people who have chosen to pay money no to see ads?

The idea of paying to go ad free may be attractive to many on the face of it, but given that an estimated 10-15% of users have an ad blocker (source: Quora), it seems that not all users want to block ads.

However, if ad blocking, paid or otherwise, does become a major concern, then advertisers need to ensure that their communications are not perceived to be annoying, intrusive messages.

Tactics for this include focussing more on content, in the way that luxury brands do, with newsworthy and enjoyable mini films, being 'useful' to the audience (like Lowe's DIY tips on Vines), and using targeting to ensure that ads are as relevant as possible.

Future Trends? What about those business opportunities that arise from future threats?

By Tamara Jacobs, Blinkx Media

It is common within every industry to reflect on the past and predict what trends will pave the way for a successful future.

Those with very strong strategic vision might take it one step further. They will look at the problems currently facing their industry and anticipate what tools might be needed to provide future solutions. Moreover, they will anticipate future threats that might result from future trends and start planning those more long-term solutions.

The digital industry is no different. In fact, given its fast evolution, it finds itself running into unforeseen obstacles more than most.

Online video for example, has grown to become a huge part of the digital industry. People love watching and sharing videos online, which makes room for aspiring and established filmmakers, producers and distributors. With so much video content being watched online, these destination sites also offer a lot of opportunity for brands to advertise around relevant content. What we have seen take place in recent years however, is a surge of unverified traffic.

And so the likes of fraud detection and verification tools spring up within the marketplace. Suddenly major players, agencies, trading desks and more are partnering with the likes of Forensiq, IAS, and Nielsen. The marketplace becomes saturated with tools that offer the solution to a problem holding back the progress and commercial opportunities of an otherwise straightforward business model.

So looking ahead at 2015, what are some of the possible business opportunities that might speak to existing or future industry threats?

Experts are considering big-ticket issues such as cross-border commerce evolving as consumers are becoming more confident to shop online. We will see an increase in retailers investing in cross-border logistics.

In the growing sector of data, it has been predicted that 2015 will produce more online data than we are able to store, what evolution in storage capabilities will answer this need?

And what about drones and their expectation to expand the aerial viewing market by £600m this year? What will they do for security? How will they be regulated within existing air space? How might they advance journalism and keep more reporters safe?

These are only but a few of the areas that entrepreneurs should be keeping an eye on, to anticipate where things will go, what could possibly go wrong and what commercially viable business opportunities might need to be readily available to adequately respond to them.

It's an important approach that a lot of people overlook. After all businesses, like anything else, are flawed. A more efficient way of doing something might spring up but it could very well lack a key component to meet consumer demands or out-win the competition, and so a second tool is required, and so on and so forth. In the most recent and most horrific financial crisis of 2008, a few leading financial geniuses saw the crash coming, prepared in silence and actually benefited from an event that turned the world on its head. I am very excited to see which forward-thinking companies and individuals will be equally strategic and impressive in the digital space moving forward.

The True Extent of Ad Fraud and the 2015 Action Plan

Juliette Gilligan, Adludio

The focus on 'viewability'[1] for a large part of 2014 overshadowed a more fundamental question about who is viewing your digital advertising in the first place – is it a human or a bot? After all, technical measures of viewability do not ensure humanity.

Last year ended with a bang – in December 2014 it was announced that at current bot rates, advertisers will lose approximately $6.3 billion globally advertising to bots in 2015.[2]

It is widely reported that over 50% of web traffic is bots. If up to 50% of what you're paying for is fraudulent, it hurts performance, reduces ROI and makes the digital advertising space less attractive for us all. According to IAB UK, digital is the single biggest advertising medium in the UK representing 39% of a £8.87 billion market and showing 6.3% year on year growth[3], so why are we not investing in the necessary bot detection security to ensure efficient use of adspend?

A flurry of press coverage surrounded the release of a report published by the Association of National Advertisers (ANA) who partnered with White Ops, a New York-based web security investigator, to determine the level of bot fraud occurring across the digital advertising industry. The report highlighted the alarming severity of a widespread problem that has penetrated the online advertising supply chain as a whole.

I felt compelled to write this article, not only to raise awareness among the key industry stakeholders about how and where bots operate, but also to highlight the tactical recommendations in the action plan so that we take the responsibility to work together to reduce and eliminate this threat.

Below are some of the top-level findings:

- The vast majority of bot traffic comes from everyday computers that have been hacked - Largely using residential IP addresses, bot traffickers remotely control home computers to generate ad fraud profits.

- Ad bots defeat user targeting - By using the computers of real people and hijacking their identity to conduct ad fraud, the bots do not just blend in - they get targeted.

---

[1] A served ad impression can be classified as a viewable impression if the ad is contained in the viewable space of a browser window - in part, entirely or based on other conditional parameters such as time and pixel requirements. Source: Viewable Ad Impression Measurement Guidelines, prepared by 'MRC in collaboration with IAB Emerging Innovations Task Force, 26 March 2014

[2] The ANA partnered with White Ops, a security company with experience eradicating ad fraud on an initiative to determine the level of bot fraud occurring across the digital advertising industry. The ANA recruited 36 member companies to participate. The participants worked with a wide variety of agency partners, including media agencies, full-service agencies, and in-house agencies.

[3] IAB / PwC Digital Adspend H1 2014 & WARC, October 2014

- **Higher CPM campaigns are most under threat**
  Like most criminal activity, ad fraudsters are opportunists following the money – thus they are attracted to higher CPM campaigns.

- **Video: Bots accounted for 23 percent of all video impressions observed[4]**
  Given that video is more expensive than display, it is more lucrative for cybercriminals. The Malware needed is also much more sophisticated - running full browsers with plug-ins and have the ability to play full videos.

- **Display: Bots accounted for 11 percent of all display impressions observed[5]**
  Less sophisticated bots have also colonised social and display, where the buys are generally cheaper and performance-based.

- **Programmatic and retargeted inventory:** Bot traffic in programmatic inventory averaged 17 percent. Bots consumed 19 percent of retargeted ads[6].

- **Mobile:** despite its rapid growth, in the bigger picture mobile currently only represents one fifth of all digital advertising[7], and therefore is less lucrative for bots. As a consequence, mobile is least affected by bot fraud but this may not be the case for long with such rapid advancement in the sophistication of cyber fraud.

What roles do the key stakeholders play?

What roles do the advertisers, agencies and publishers play and whose responsibility is it to take ownership of the problem? The truth is that this is an industry-wide threat that is infiltrating the advertising supply chain, as a whole; advertisers, agencies and publishers are all victims, although arguably some have more to lose than others. The threat to the advertiser's ROI from advertising to bots is the most obvious sore spot. That said it is in a publishers best interest to offer clean inventory to protect its business reputation, which has an intangible impact on its financial wellbeing. Especially given the findings in the report that significant bot levels affected all tiers and types of publishers, despite premium Tier 1 classifications, so it is all to play for.

[4] The ANA partnered with White Ops, a security company with experience eradicating ad fraud on an initiative to determine the level of bot fraud occurring across the digital advertising industry. The ANA recruited 36 member companies to participate. The participants worked with a wide variety of agency partners, including media agencies, full-service agencies, and in-house agencies. White Ops tagged participants' creative in August and September 2014 (181 U.S. campaigns) to determine fraud activity. The study measured 5.5 billion impressions in 3 million domains over 60 days.

[5] As per footnote 4

[6] As per footnote 4

[7] IAB / PwC Digital Adspend H1 2014 & WARC, October 2014

What's the action plan?

It is imperative for the key stakeholders to collaborate to combat fraud while independently taking responsibility to implement their own action plan. See the top tactical advice below as recommended by the ANA in conjunction with White Ops. In all, 17 recommendations were put forth.

Action plan for buyers:

1. Monitor all traffic with a consistent third party tool to allow for comparability. This can validate or disprove assumptions about the quality of a publisher or ad tech company's traffic, despite its premium classification. It is recommended to use monitoring and bot detection to reveal the bots in retargeting campaigns and audience metrics. This will prevent the purchase of additional media targeted at those bots and will improve campaign metrics.

2. Update blacklists frequently and narrowly – as often as daily and control for ad injection (the unauthorised placing of ads on sites where they do not belong can cause programmatic buys to contain higher levels of fraud) by discussing this with your DSP or tech platform.

3. Concentrate advertising during audience waking hours and reduce buys on older browsers. Bot fraud levels vary across the day with peak activity occurring when users are sleeping, but their computers are still awake, between midnight and 7am. Additionally, fraudulent impressions coming from older browsers were significantly higher (such as IE6 and IE7).

Action plan for publishers:

1. Continuously monitor sourced traffic - know your sources and maintain transparency about traffic sourcing. Eliminate sources of traffic that are shown to have high bot percentages. Monitor all vendors, all the time.

2. Protect from content theft and ad injection - Use a service such as domain detection or bot detection to monitor for content scraping (presenting another site's content in a separate website and monetising the scraped content with ads) and evidence of ad injection. A bot detection service can measure actual numbers of bots in high-bot traffic, allowing payment for the human audience while eliminating bots from the billing process.

3. Authorise third party monitoring to enable advertisers to improve the granularity of their traffic performance (such as viewability, engagement, and bot detection) and third-party tracker measurement.

What we can expect in the year ahead:

This year we will see propositions from ad tech companies that eliminate impression fraud, click fraud, affiliate fraud and cookie stuffing come to the fore. I think the first actionable result will be in the form of financial adjustments being made post-campaign based on delivery reports. Enter Cost Per Human (CPH), a pricing model that measures the actual cost of human impressions after accounting for loss due to ad fraud. Ultimately I think that buying custom

'pre-cleansed' inventory at a campaign level will become the 'new normal' for advertisers.

In summary, the industry wide preoccupation with viewability has detracted focus from the alarming extent of online ad fraud. It is time to take the responsibility to develop an understanding of this issue that has emerged over the past few years as it poses a genuine threat to the sustainability of the advertising ecosystem as we now know it. Advertisers, and all industry participants can and must take action.

Players that authorise third-party traffic validation technology, and implement the recommendations set out above to immediate effect to combat ad fraud will be the pioneers in this space. The winners, however, will be the brands, as they will finally see their digital budgets put to efficient and effective use – advertising to humans, not bots.

The Future's Bright

Alison Sprague, CEG Europe

The future is bright. At least that is what all the signs are indicating. The number of first time house buyers rose by 22% in 2014, hitting its highest level since 2007.[8] The UK car industry started the New Year on a high, with figures revealing that there was a record run of sales growth of 34 consecutive months and 2014 registered as the best annual retail performance for a decade.[9] Add in some reasonably optimistic GDP projections for 2015 and the projection by Group M that online spend is forecast to grow 12.7% year-on-year to break the £8bn mark.[10] As Ofcom recently reported, the UK's internet economy is one of the strongest in the world.[11] What could possibly stand in the way of a thriving internet advertising industry in 2015?

Regulation? Regulation always has a fixed cost – understanding and navigating the relevant rules and regulations, keeping abreast of any changes or new proposals and ensuring compliance. The charts below provide a high level summary of the main areas involved, together with the principal stakeholders that initiate and, in some cases, monitor regulation.

Overview of online advertising rules and regulations

Data protection	Privacy	Consumer protection
Advertising rules and regulations		
Legal, decent, honest	Directed at children	Transparency
Sector specific e.g. alcohol	Behavioural advertising	Pricing

The recent Oreo vlogging case is a prime example of how advertising rules and regulation are applied online. The ASA banned a campaign for Oreo biscuits featuring YouTube stars that did not clearly label the videos as having been paid for. The ASA stated: "Ultimately, it pays to be honest … It's important to note that, if advertisers and vloggers aren't upfront, not only could they be in breach of the Advertising Code, they could also be breaking the law."[12]

[8] See: http://www.bbc.co.uk/news/business-30684286

[9] See: http://www.ft.com/cms/s/0/1d8f2858-95fc-11e4-a390-00144feabdc0.html

[10] This would make the UK the first country in which more than £1 in every £2 of ad spend is on digital media. See: http://www.theguardian.com/media/2014/dec/01/gadget-obsessed-uk-top-digital-advertising-spend

[11] http://consumers.ofcom.org.uk/news/importance-of-uk-internet-economy-revealed

[12] http://asa.org.uk/News-resources/Media-Centre/2014/Making-ads-Clear-The-challenge-for-advertisers-and-vloggers.aspx

Stakeholders involved in developing and monitoring online advertising regulation

The industry – self regulation

The stakes can be higher than getting a campaign banned if you don't adhere to the rules and regulations. First you can get reported - to the ASA, Trading Standards and/or the UK's new competition authority, the Competition and Markets Authority. Depending on the nature of the rules breached, you could be fined, prosecuted or imprisoned. As well as the rules and regulations, compliance with the law (see below) is a must.

Relevant law

The Consumer Protection from Unfair Trading Regulations 2008 (CPRs)
The Unfair Terms in Consumer Contracts Regulations 1999 (UTCCRs)
The Consumer Protection (Distance Selling) Regulations 2000 (DSRs)
Enterprise Act 2002
Data Protection Act 1998
Privacy and Communication Regulations 2011

A renowned case is the OFT's own-initiative investigation into Groupon following complaints about its trading practices. The OFT found that a number of Groupon's trading practices:

> "...appeared to be in breach of the CPRs, the UTCCRs and DSRs. In particular, OFT identified concerns with reference pricing, advertising, refunds, unfair terms, and the diligence of its interactions with merchants."[13]

The OFT closed the case once Groupon, which was reported to have engaged constructively and cooperated throughout the investigation, signed specific undertakings. The undertakings were deemed as standard setting for the sector – the OFT sent them to a further 35 daily deal companies. The case indicates that the threat of reputational damage and the possibility of fines is a strong deterrent to playing ignorant in this space.

So what may be new this year? A quick scan of annual plans of several of the principal stakeholders reveals little. Industry led self-regulation of targeted behavioural advertising appears to work well – there's no reports of any future industry-wide investigations following the conclusions of the OFT's Online

[13] See: http://webarchive.nationalarchives.gov.uk/20140402142426/http:/www.oft.gov.uk/OFTwork/consumer-enforcement/consumer-enforcement-completed/groupon/ - named7

Targeting of Advertising and Prices Market Study. Data protection of course remains a challenge as we await full agreement on the proposed EU directive with hopefully its scope being manageable and proportionate and in particular the "pseudonymous data" issue resolved. As IAB UK states: "it is very likely that businesses will have to make adjustments to their operations as part of complying with the future law."[14]

While that may come as a cost, hopefully most will have addressed this in previous years.

Online video content marketing, while gaining popularity, remains a tricky area and there is a view that traditional media (essentially TV) will want the playing field levelled.[15] In TV, advertising content and editorial are strictly separate. The Oreo case indicates that the ASA is keeping a watchful eye so perhaps caution may stall this avenue of advertising. There may be a case for kite-marking here. While compliance with regulation may be perceived as a cost, it can be seen as a benefit – if consumers are aware of self-regulatory/ kite-marked good practices then trust is enhanced. Aside from the still unresolved data protection directive (which given the delays has enabled everyone to get up to speed with the core requirements) it appears that future regulatory barriers are unlikely.

But of course there's always a possibility given the continual rapidly changing technology that something new may be developed and battles between the compliance, marketing and technical departments may commence. Best to ensure the battles remain in-house and get resolved before hitting the internet.

[14] See: http://www.iabuk.net/policy/briefings/ec-data-protection-reforms-briefing-for-iab-members-1

[15] See: http://www.theguardian.com/media-network/olswang-partner-zone/2015/jan/14/content-marketing-native-advertising-regulation