

Date 13 March 2018

**Re: industry support for the Parliament's ePrivacy Regulation text, with minor amendments.**

Dear Colleague,

I write to support the proposed ePrivacy Regulation, which with minor a amendment is an important contribution to the regulation of online advertising. I represent PageFair, a European advertising technology company based in Dublin. PageFair works with publishers across the globe to display several billion online ads per month.

PageFair enjoys a thought leadership position in the online media industry: thousands of adtech and online industry professionals analysts subscribe to receive our research notes on issues in the online industry. Our reports are cited in The New York Times, The Economist, The Financial Times, Wired, and other major publications.

We support the Commission's proposal, and the Parliament's text, where they concern web and mobile advertising. Our remarks are tightly bounded by our expertise in online advertising technology. We do not have an opinion on how the proposed Regulation will impact other areas. We applaud the introduction of "Do Not Track" privacy protections, end-to-end encryption, and maintenance of the high consent standard of the GDPR, and prohibition on cookie consent walls. In particular, **we applaud the Parliament's 96th and 99th amendments**, concerning Article 8. These are essential to enable standard Internet Protocol connections to be made in many useful contexts that do not impact of privacy.

The protection of fundamental rights to privacy and data protection enshrined in the Charter is compatible with sophisticated advertising technology. It is with this in mind that we propose an amendment to permit privacy-by-design advertising. As a growing global business based in Europe, we believe that the proposed Regulation will enable digital businesses to flourish in the longer term - provided the following minor amendment is made to Article 8.

## Proposed amendment to Article 8 to allow privacy-by-design advertising

Article 8 of the Commission's proposal prohibits processing and storage of information on end-users' terminal equipment. This applies even to information that is not related to interpersonal communications services, or to personal data. **As drafted, this will prevent websites from displaying privacy-by-design advertising that advertisers are willing to pay publishers for.**

Therefore, we propose an exception should be added to Article 8 that allows terminal storage for the purposes of contextual advertising techniques, and the campaign measurement that advertisers require, provided these neither generate nor reveal personal data or information related to an interpersonal communications service. This is essential to enable publishers to transition from tracking to advertising that does not track individuals but is still relevant. **Such advertising techniques pose no risk to confidentiality of personal communications or to personal data, and will allow a vibrant and plural media to remain freely accessible in the Union.**

We have discussed this proposed amendment with various colleagues in the online media and advertising industry, who agreed on the privacy-preserving character our suggested proposal. The text we propose is below.

Add an exception to Article 8, paragraph 1:

“if it is technically necessary for contextual advertising techniques and reporting, provided neither personal data, nor information related to an interpersonal communications service, nor unique IDs, are created nor processed.”

Recital 21 should define contextual advertising techniques and reporting to facilitate application of these rules in practice, and neutralise any risk of opening a loophole for tracking. The following should be added to Recital 21 (after the discussion of “measuring web traffic” and before the discussion of “configuration checking”):

“This may also include storing for a limited time information for privacy-friendly and relevant advertising, such as topics of interest related to content accessed by users, and simple statistical counts of advertising campaign impressions, provided that the topics of interest are not special categories of data, and that result of the processing is not personal data, but aggregate data, and that these data cannot be used to single out any particular natural person”.

Provided this exception is added, the ePrivacy Regulation as proposed will be an important spur to innovation in our industry.

## Tracking is not necessary for the online advertising & media industry to thrive

There are significant harms associated with online behavioural advertising. Every time a behaviourally targeted ad is served on a website, the system that selects it leaks personal data to hundreds or thousands of companies.<sup>1</sup> These personal data include the URL of every page a user is visiting, their IP address (from which geographical position may be inferred), details of their device, and various unique IDs that may have been stored about the user previously to help build up a long term profile about him or her.

This is a vast, often intentional, and ongoing data breach. Our industry has built no adequate controls to enforce data protection among the many companies that receive data.

The economic benefit of behavioural tracking to publishers is arguable. IAB Europe, an adtech/targeting industry trade body,<sup>2</sup> recently funded a study on “The economic value of behavioural targeting in digital advertising”. Figures from this study show that behaviourally targeted advertising accounts for only a quarter of European publishers’ gross revenue.<sup>3</sup>

The most lucrative forms of revenue generation for larger publishers is “directly sold” advertising, which brings much higher revenues per ad seen, by a factor of 200% or more,<sup>4</sup> than behavioural ads. Advertising networks are available to smaller publishers.

The behavioural targeting industry often demonstrates the value of its product by examining how much its ads earn from automated bids in online ad auctions. This is redundant, since the market post-GDPR will not generally contain personal data. One

---

<sup>1</sup> See “Data leakage in online advertising”, PageFair, September 2017 (URL: <https://pagefair.com/data-leakage-in-online-behavioural-advertising/>); and Steven Englehardt and Arvind Narayanan, “Online tracking, a 1 million site measurement and analysis”, Princeton Web Census, 2016 (URL <https://webtransparency.cs.princeton.edu/webcensus/>); and *Data Brokers: A Call for Transparency and Accountability*, The Federal Trade Commission, 2014 (URL: <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>).

<sup>2</sup> PageFair is a member of IAB UK and of IAB Tech Lab in the United States.

<sup>3</sup> See *The economic value of behavioural targeting in digital advertising*, IAB, 2017. Particularly note footnote 2 definition of “display” advertising. The quarter figure is calculated as follows, using the IAB-funded study’s numbers: While online advertising accounts for €41.9 billion in gross revenue to publishers, only only €16 billion of this is not classifieds or search advertising, and of this €16 billion, only €10.6 billion is from “behavioural” advertising that relies on personal data.

<sup>4</sup> Based on consultations with several publisher trade groups.

would not predict the value that electric vehicles will have after a carbon regulation is introduced by walking into a car showroom before the regulation and comparing their current price to petrol equivalents.

And yet, it is worth dispelling the latest such study, funded by IAB Europe. It compared the revenue created by behaviourally targeted ads to the most basic form of online advertising (“run-of-network” ads). This is not a genuine comparison.<sup>5</sup> But even if better comparisons had been used, these studies are problematic because behavioural advertising is plagued by “ad fraud”, where software bots masquerade as human Internet users by viewing and clicking on ads to defraud advertisers of their budgets. This happens at a massive scale, estimated by the main advertisers’ trade body to cost \$150 Billion by 2025.<sup>6</sup>

The value of behavioural targeting to advertisers is also challenging to evaluate. The trading of behavioural advertising through automated auctions has introduced a complex of middle-men, which absorb the majority of the revenue. For example, when *The Guardian* bought ads on its own site through an auctioning system for behaviourally targeted ads, it received only 30% in revenue of the sum it paid as a buyer.<sup>7</sup> As *The Guardian* discovered, ad tech parties take roughly 70% of all revenue in behavioural advertising.

Finally, it is worth examining the industry trend in behavioural advertising. In 2017 Google and Facebook absorbed an estimated 63% of all spending on online advertising in the US market, where “behaviorally targeted advertising” is embraced more than in Europe.<sup>8</sup> Google and Facebook absorbed 93% of all revenue (net) growth in 2017. All other publishers gained only 7%.<sup>9</sup> As the recent IAB-funded study notes, an increasing percentage of European online advertising revenue is attributable to the behavioural targeting.<sup>10</sup> This is not necessarily a positive development for publishers, unless they are Google or Facebook.

---

<sup>5</sup> See *The economic value of behavioural targeting in digital advertising*, IAB, 2017, in particular note footnote 3.

<sup>6</sup> See Mikko Kotila, Ruben Cuevas Rumin, Shailin Dhar, “Compendium of ad fraud knowledge for media investors”, World Federation of Advertisers, 2016, p. 3 (URL: [https://www.wfanet.org/app/uploads/2017/04/WFA\\_Compendium\\_Of\\_Ad\\_Fraud\\_Knowledge.pdf](https://www.wfanet.org/app/uploads/2017/04/WFA_Compendium_Of_Ad_Fraud_Knowledge.pdf)). One cannot with confidence determine whether people are actually clicking on an ad, or whether some or all of these clicks are actually executed by automated “adfraud bots”, whose sole purpose is to click these ads to fraudulently charge advertisers.

<sup>7</sup> “Where did the money go? Guardian buys its own ad inventory”, MediaTel, October 2016 (URL: <https://mediatel.co.uk/newslines/2016/10/04/where-did-the-money-go-guardian-buys-its-own-ad-inventory/>) and “Guardian buys own ad inventory, only gets 30p to the pound”, Marketing Mag, October 2016 (URL: <https://www.marketingmag.com.au/news-c/guardian-programmatic-advertising/>).

<sup>8</sup> “Google and Facebook Tighten Grip on US Digital Ad Market”, eMarketer, September 2017 (URL: <https://www.emarketer.com/Article/Google-Facebook-Tighten-Grip-on-US-Digital-Ad-Market/1016494>)

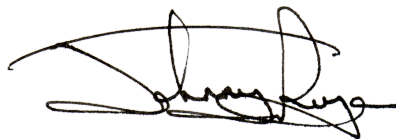
<sup>9</sup> *ibid.*

<sup>10</sup> *The economic value of behavioural targeting in digital advertising*, IAB, 2017, p. 2.

Tracking is not necessary. In our view - provided that Article 8 is amended as suggested in this letter - the industry can remove all personal data currently used in behavioural ads, and switch to contextual, non-personal data.<sup>11</sup> We are collaborating with major publishers and with technology partners to do so. It is not tenable for any publisher, adtech vendor, or trade body, to claim that they must persist in their current practises.

The digital economy requires a foundation of trust to enable innovation and growth. The enormous growth of adblocking (to 615 million active devices) across the globe proves the terrible cost of not regulating. We are witnessing the collapse of the mechanism by which audiences support the majority of online news reports, entertainment videos, cartoons, blogs, and cat videos that make the Web so valuable and interesting. Self-regulation, lax data protection and enforcement have resulted in business practices that promise a bleak future for European digital publishers. Therefore, we commend the Commission and Parliament's work thus far, and urge you to consider our proposed amendment to Article 8.

Faithfully,



Dr Johnny Ryan FRHistS  
Head of Ecosystem

---

<sup>11</sup> Non-personal data are any data that can not be related to an identifiable person. As Recital 26 of the GDPR observes, "the principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable". This recital reflects the finding of the European Court of Justice in 2016 that data are not personal "if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and manpower, so that the risk of identification appears in reality to be insignificant". Judgment of the Court (Second Chamber) Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14, 19 October 2016.