

10 October 2019

Re Industry support for privacy protection in an ePrivacy Regulation

Dear Colleague,

I represent Brave, a private web browser with offices in Europe and the United States. Our CEO, Brendan Eich, is the inventor of JavaScript, and co-founded Mozilla/Firefox. Our employees work on machine learning, blockchain, and private online advertising technology. Brave works with publishers across the globe.

The ePrivacy Regulation is necessary to build a foundation of trust for the digital market. However, we are concerned about two elements of the current draft.

1. We oppose “cookie walls” (Recitals 20 and 21, which accompany Article 8).

Advertising is fundamental to financing the web, but it must respect users’ rights and expectations. As technologists, we know that the rights to privacy and data protection enshrined in the European Charter are compatible with innovation. Many companies, including Brave, have developed advertising systems that support publishers with no privacy sacrifice. A robust ePrivacy Regulation will spur further innovation.

But as currently drafted, the text permits “cookie walls” that make pervasive tracking a condition of access to a website. EU data protection authorities have good reason to regard such cookie walls as unlawful.¹

Cookie walls would not serve the economic interests of publishers, as the latest research makes clear.² Recitals 20 and 21 allow cookie walls that facilitate “real-time bidding” behavioural advertising. But this system is economically inefficient,³ rife

¹ “Guidelines on consent under Regulation 2016/679”, Article 29 Working Party, updated April 2018 pp. 8-10.

² “Veronica Marotta, Vibhanshu Abhishek, Alessandro Acquisti, Online Tracking and Publishers’ Revenues: An Empirical Analysis” The 2019 Workshop on the Economics of Information Security (URL: https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf); see also “Major publisher group DCN tells regulators “the sky won’t fall” if RTB switches to safe, non-personal data”, Brave Insights, 19 June 2019 (URL: <https://brave.com/dcn-letter-rtb/>).

³ The Guardian purchased advertising on its own web site as a buyer, and received only 30% of its spend as a supplier. See “Where did the money go? Guardian buys its own ad inventory”, Mediatel Newslines, 4 October 2016 (URL: <https://mediatel.co.uk/newslines/2016/10/04/where-did-the-money-go-guardian-buysits-own-ad->

with fraud,⁴ provides the business model of disinformation,⁵ and is responsible for the largest data breach ever recorded.⁶

Google and IAB Europe, which control the “real-time bidding” ad industry, are both under investigation by their lead authorities under the GDPR for precisely the same practices that would be facilitated by cookie walls.⁷ Indeed, these practices very recently made front page news in *The Financial Times*.⁸

Competition authorities in several Member States are examining the problems of the online advertising and media market caused by these same practices.

2. We believe that Article 10 should be reinstated to protect privacy by default.

Public trust in how data is handled has been damaged by scandals such as Cambridge Analytica. The ePrivacy Regulation should contribute to rebuilding that trust rather than perpetuating the business practices which undermine it.

inventory). The tracking industry’s own trade body notes that publishers receive only 45% of every Euro spent by advertisers in the online behavioural advertising system, in “The Programmatic Supply Chain: Deconstructing the Anatomy of a Programmatic CPM”, IAB, March 2016 (URL: <https://www.iab.com/wp-content/uploads/2016/03/Programmatic-Value-Layers-March-2016-FINALv2.pdf>). In other words, publishers appear to receive only 45% - 30% of money spent by advertisers in Europe’s €16B “RTB” online advertising market. The 30% figure is from an investigation by

⁴ “Ad Fraud To Cost Advertisers \$19 Billion in 2018, Representing 9% of Total Digital Advertising Spend”, Juniper Research. September 2017 (URL: [https://www.juniperresearch.com/press/press-releases/ad-fraud-to-cost-advertisers-\\$19-billion-in-2018](https://www.juniperresearch.com/press/press-releases/ad-fraud-to-cost-advertisers-$19-billion-in-2018)).

⁵ “The Quarter Billion Dollar Question: How is Disinformation Gaming Ad Tech?”, Global Disinformation Index, September 2019 (URL: https://disinformationindex.org/wp-content/uploads/2019/09/GDI_Ad-tech_Report_Screen_AW16.pdf); see also testimony of Jason Kint, CEO of publisher tradebody Digital Content Next, at the International Grand Committee hearing on big data, privacy, and democracy, 28 May 2019; see also Johnny Ryan speech at the European Data Protection Supervisor “Europe votes” conference, February 2019 (URL: <https://vimeo.com/317245633>).

⁶ As the UK Information Commissioner recently noted: “one visit to a website, prompting one auction among advertisers, can result in a person’s personal data being seen by hundreds of organisations”, in “Update report into adtech and real time bidding”, Information Commissioner’s Office, 20 June 2019, pp 3-4 (URL: <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf>). See also “Regulatory complaint concerning massive, web-wide data breach by Google and other “ad tech” companies under Europe’s GDPR”, Brave Insight, September 2018 (URL: <https://brave.com/adtech-data-breach-complaint/>). For the scale of the data breach, see “Count of hundreds billions of bid request broadcasts”, evidence submitted to data protection authorities in UK & Ireland (URL: <https://brave.com/wp-content/uploads/2019/07/Scale-billions-of-bid-requests-per-day-RAN2019061811075588.pdf>).

⁷ See “Data Protection Commission opens statutory inquiry into Google Ireland Limited”, Data Protection Commission of Ireland, 22 May 2019 (URL: <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-opens-statutory-inquiry-google-ireland-limited>); and letter from Peter Van den Eynde of the Gegevensbeschermingsautoriteit to Jef Ausloos and Pierre Dewitte, 8 October 2019.

⁸ For example, see “Google accused of covertly passing users’ personal data to advertisers”, *The Financial Times*, 5 September 2019, front page.



Users should be able to trust their software not to disclose personal data without consent. Research shows that users rarely modify their settings,⁹ which is why the choice of defaults is fundamental.

We urge the Working Group to take this into account in its deliberations. I am happy to brief you further on these issues.

Yours sincerely,

A handwritten signature in black ink, appearing to read "Alan Toner". The signature is fluid and cursive, with the first name "Alan" being more prominent than the last name "Toner".

Alan Toner
Policy Expert
Brave

cc

Roberto Viola, Director General, DG Connect
Birgit Sippel, MEP

⁹ Jared spool, "Do Users Change their Settings", UIE, September 2011 (URL: <https://archive.uie.com/brainsparks/2011/09/14/do-users-change-their-settings/>).