Response to
"CMA Online platforms and digital advertising market study – Statement of Scope"

Respondent:

Michael Barwise
Business Information Risk Management Consulting (BusinessInfoRisk.co.uk)
6 Maple Green, Hemel Hempstead, HP1 3PY
consulting@businessinforisk.co.uk
0845 463 1624

Responding as a business

No restrictions on dissemination

Further discussion invited

Business Activities:

Consultancy services to organisations on information risk, including privacy management and compliance with data protection legislation

Expert contributions to national and international information risk initiatives

Response

Proposed scope

The scope of this study, as currently limited to platforms funded by digital advertising, apparently fails to address a significant problem. While it clearly recognises data collection via direct interaction of individuals with a platform (e.g. searching on Google or posting and browsing on Facebook), it seems to ignore widespread cumulative data collection by platforms resulting from involuntary indirect interaction with them in the course of using online services that are not necessarily funded by advertising. This is of particular concern where services deploy tracking devices that automatically and covertly communicate with such platforms.

For example, a report[1] published in March 2019 uncovered *"[...] evidence of widespread systematic tracking by the ad tech industry on government websites that are not funded by ads."* The report makes an important point in suggesting that the publishers might have been unaware that third party functionality they included in the sites for apparently legitimate reasons contained tracking technologies. This strongly suggests both a knowledge deficit and a lack of due diligence on the part of publishers. We therefore consider the scope of this study should be widened to address the use of tracking where the party deploying it is not a platform that is the ultimate recipient of the data.

The right of individuals to actually control, rather than merely be informed of, data collection and processing by platforms seems under-emphasised in the current scope. Phrases such as "consumers getting insufficient compensation for their data" in paragraph 63 and "consumers receiving poor value for their data" in paragraph 65 appear to imply an assumed acquiescence to data collection based on some undefined but universally acceptable quid pro quo. We dispute this premise. Ideally an individual should be exempt from having their data collected for advertising purposes except with their explicit informed consent or where they have voluntarily engaged directly with the platform that ultimately collects the data. We therefore consider the scope of this study should be widened to address ways of ensuring the default is exemption from tracking where the relationship with a platform is indirect (via a publisher), and particularly where the individuals concerned are potentially unaware that such tracking is taking place.

[1] https://www.cookiebot.com/media/1136/cookiebot-report-2019-ad-tech-surveillance-2.pdf

Theme 1

No comments.

Theme 2

Issues

The use of automated covert third party tracking elements on web sites has reached epidemic scale. They have been found even where site content is sufficiently sensitive that records of access to the site could constitute sensitive personal data under Article 9 of the GDPR.[2] This would necessitate the data collector obtaining freely given, specific, informed and unambiguous consent at the time of collection, and provision for withdrawal of that consent. It is, however, not clear how such consent could be managed in the case of automated covert data collection.

Cookies, hidden images and JavaScript are the most prevalent tracking mechanisms. The controls over these offered by current web browsers are “all or nothing”, and as current practice in web design may make legitimate use of all these technologies, using the existing controls to block trackers can have the side effect of preventing or restricting access to the content of a web site.

Third party extensions offering finer control have emerged for selected web browsers, and it is possible that comparable functionality could be built directly into browsers themselves in the future. However their proper use requires a level of knowledge and understanding substantially beyond that of the general public. It also is worthy of note that two of the leading browser providers are themselves also platforms that gather personal data for advertising purposes, so the degree to which their controls might provide protection from that data collection is open to question.

Some platforms do provide for “opt out” – typically by setting a cookie – but that usually requires direct voluntary interaction with the platform itself. Consequently an individual wishing not to be tracked via a publisher has to be aware they have been or are being tracked and be able to identify the tracking platform (both of which are unlikely where covert tracking via a publisher is in use). They must also enter into a direct relationship with the platform to avoid having a relationship with the platform, which presents something of a conundrum.

Thus we see that, specifically where tracking is indirectly conducted via a publisher, user control over collection of their data by platforms is at present essentially illusory.

It is clear from the above that platforms funded by digital advertising per se are by no means the sole, or even the main, source of cause for concern. In quite possibly the majority of cases of tracking, there is no direct, conscious or intentional relationship between the individual and the platform ultimately collecting their data. The individual may often not even know to whom to apply to object to being tracked, let alone being informed by the platform of the collection, as is the data subject's right under Article 14 of the GDPR.. This situation should be given serious consideration as it represents significant intrusion into the private lives of vast numbers of individuals – even those who actively desire to avoid interacting with the platforms.

Remedies

We do not consider that technological solutions such as enhanced browser controls are a panacea, or probably even a primary solution. The issues at stake are not static, but constitute a fast moving continuum of cyclic action and reaction between those advocating privacy and those seeking to exploit personal data on an international scale. As fast as protections are introduced, attempts are likely to be made to circumvent them. Furthermore the conflict of interest where a platform is also a browser provider will always make the efficacy of protections in those browsers questionable.

We consider that legislation and regulation alone are probably insufficient. Regulation as suggested in paragraph 92 can only be justified if enforcement is practicable and effective. Given that the major advertising platforms are transnational, enforcement will represent a

[2] ibid

significant challenge. In addition to jurisdictional problems of enforcement, the disparity between ideals of privacy and the demands of probably the most profitable global industry is so vast that adequate compromises are unlikely to be reached in the foreseeable future. There is indeed a danger of apparently far reaching but practically toothless legislation being passed that achieves no useful outcomes despite satisfying perceptions (as exemplified by the widespread abuse of the "legitimate interest" basis of the GDPR). Consequently, we consider that national legislation is likely to be effective only if it concentrates on the local and smaller scale rather than the global and larger scale aspects of personal data gathering. It should preferentially address the activities of publishers where the disparity of power between the parties is minimal, rather than those of platforms where it is disproportionately great.

Therefore, rather than primarily relying on technologies or attempting to regulate platforms directly, more might be gained by creation of practical guidance for businesses making use of advertising platforms. Such guidance is particularly important for web service developers, who are frequently given a free hand to include what they see fit on a site, but whose lack of understanding can render a web site owner unwittingly responsible for inappropriate data collection (see Appendix). If clear guidance to those creating and operating web sites can reduce demand for an excessively intrusive platform's services, there may eventually be a commercial imperative to rectify it.

We consider that for maximum effectiveness such guidance should not be expressed in terms of legal obligations (as is typical of much guidance currently produced by the ICO) as this tends to confuse those without legal training. It should instead be intensely pragmatic, even to the extent of being presented as detailed "do" and "don't" checklists, sufficiently clear and detailed not to require interpretation by technical or legal specialists. We believe that most web site owners do not intend to facilitate inappropriate collection of personal data, but that they are mostly unaware, or are influenced directly or indirectly by transnational advertising platforms that have a vested interest in data collection and may view that interest as overriding the rights and freedoms of individuals.

Most importantly, public awareness should be addressed. The huge popularity of extremely intrusive social networking services demonstrates the current paucity of understanding about the extent to which personal data is trawled. Accurate information about the degree to which web users are tracked and profiled, and the potential consequences thereof, could ultimately have a major influence on public opinion. However the information must be presented in a manner that neither induces denial though fear nor under-emphasises the extent of the problem. Any resulting change in public opinion could contribute to curbing excess collection of personal data in aid of online advertising.

In summary, we see the most significant problem as the vast number of web sites that automatically and often covertly indirect personal data to advertising platforms, rather than as direct data collection by the platforms themselves via individuals directly and voluntary interacting with them. The study would be less than useful should it not include consideration of this issue.

Theme 3

No comments.

Appendix

A judgement[3] of the Court of Justice of the European Union dated 29 July 2019 holds that a publisher deploying a platform's tracker is a joint Data Controller with the platform "*[...] in respect of the operations involving the collection and disclosure by transmission [...] of the data at issue*". The Court considered that the publisher is not a joint Data Controller for any subsequent processing conducted by the platform.

2019-07-29

END

[3] https://curia.europa.eu/jcms/jcms/p1_2278332/en/