Response to
"CMA Online platforms and digital advertising market study interim report'

Respondent:
Michael Barwise
Director
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

18) Do you agree we have identified the right areas for further work in the second half of the study (set out below), and are there any significant gaps?

Not entirely

Unnecessary covert third party tracking
The dominant emphasis of this report on search engines and social media platforms, with both of which the user typically engages voluntarily, ignores a much wider user loss of control over personal data resulting from the inclusion of covert tracking on a very high proportion of web sites, even where it does not necessarily support monetisation or advertising. There are numerous instances of this where the tracking is implemented by a third party service employed by the principal rather than by the principal itself (e.g. on the ICO jobs microsite[1]), or where third party web developers include trackers on their own initiative on commissioned web sites. In either case, the principal has a statutory duty to ensure that the privacy of users of the site is respected, and by implication a duty to ensure that any such tracking is either explicitly disallowed or justified by a declared legitimate purpose and managed in accordance with the law. However the currently typical enforced consent, e.g. "by continuing to use this web site you agree &c." and a generally observed failure to distinguish between the "strictly necessary" class of "cookie" defined by PECR and tracking entities indicate both the serious nature of the problem and the inadequacy of current enforcement.

Privacy policies as a control
Our continuing research into the adequacy of privacy policies indicates that for the most part they are seriously deficient and do not fulfil the transparency intent of current EU or UK legislation. They frequently do not provide sufficient information in sufficient detail to allow the exercise of data subject rights. A particular case is the right to object to processing on the basis of legitimate interest, which has emerged as the dominant catch-all basis for the use of analytics and advertisement-related tracking. However, purposes reliant on this basis are usually expressed in such vague terms (e.g. "to improve our web site") that no clear argument can be established to raise an objection. As, furthermore, the arbiter of the validity of an objection is the web site owner, this is a significant source of user exposure that has little chance of redress. Typically, objections are ignored or the objector is bounced back and forth between the principal and the third party providing the tracking service, and the ICO typically does not pursue single complaints by individuals of what could be construed on the global scale as minor regulatory breaches, but are nevertheless to the individual significant infringements of their rights.

[1] https://www.theregister.co.uk/2019/11/07/ico_jobs_microsite_set_hundreds_of_cookies_without_consent/

Furthermore, businesses that gain materially from tracking and profiling will inevitably attempt to steer as close to the letter of the law as they can to maximise their freedom of action. Consequently, privacy policies and the enforcement of their compliance with the legislation as currently practiced can not in practice be relied on as a control.

Browser settings as a control

We consider that reliance on browser settings as a primary or main privacy control is entirely the wrong emphasis, as it forces the individual web user into a permanent defensive posture. This is no different in principle from asserting that everyone should wear a bullet proof vest to protect themselves from being shot. In any case, regardless of assertions to the contrary by platform owners, assiduous efforts are continuously under way to circumvent browser based privacy controls. They therefore provide no permanent assurance of efficacy, and their current state of effectiveness is generally an unknown to the user.

Cost/benefit balance to persons not voluntarily engaging with tracking and profiling platforms

The general thrust of the report appears to be that activities of which only around 15% of the public approve[2] are in principle essential in support of a public good that should be encouraged to persist. We strongly disagree. There is a significant danger that both web using members of the public and advertisers are merely becoming pawns in the process of revenue generation by advertising service providers and that such providers could thus be seen as essentially parasitic. Although hugely profitable to their providers, these services have still neither been conclusively shown to be proportionately advantageous to advertisers compared with contextually placed advertising that does not require viewer profiling, nor to be proportionately beneficial to the targeted public in view of the intrusiveness of the tracking and profiling on which it relies. Indeed there is significant anecdotal evidence of mis-targeting of real-time auctioned targeted advertisements, a common phenomenon being advertisements specifically promoting goods recently purchased. Such advertisements are obviously not likely to convert to sales. Equally important is the issue of relevance to the content sought by the target. Irrelevant advertisements are also unlikely to convert to sales. In neither case is either the advertiser or the public well served, although the intermediaries profit, often significantly, from it.

The overall extent of such generalised tracking and profiling is at least comparable to that carried out via platforms voluntarily signed up to by members of the public, and thus deserves at least equal, if not more, attention, particularly because it is much more difficult for the public to object to effectively or control. Consequently we consider that this generalised tracking and profiling and the potential social problems it engenders are insufficiently addressed by this report, and indeed by current legislation (due both to lack of explicit controls and to inadequate enforcement). As a matter of course it should be possible for a person to avoid, rather than merely to (typically fruitlessly) object to, online tracking, and in event of requiring to object, to be conveniently and reliably assured that their data is eradicated. Current regimes of control (including legislation as presently enforced) do not ensure these gaols are achievable. We therefore feel that the report should clearly emphasise these concerns and suggest direction for addressing them, including if necessary additional or modified legislation to curb the extent of tracking and profiling. In view of the profitability of covert tracking and profiling and the disparity of scale between those performing it and those tracked and profiled we consider that self regulation and codes of conduct will prove insufficient.

END OF RESPONSE

[2] 4.43 '[...] only 15% of respondents were happy for online companies to collect and use their data to show more relevant adverts or information[...]'