Nick Johnson Partner
nick.johnson@osborneclarke.com
Osborne Clarke LLP, London

The ePrivacy Regulation and adtech

The proposed new EU ePrivacy Regulation threatens the business models of many in the adtech sector. Nick Johnson, Partner at Osborne Clarke LLP and Member of the *Digital Business Lawyer* Editorial Board, reviews the challenges it poses and looks at possible outcomes for businesses in this space.

The European Commission's proposal for updating the ePrivacy Directive is still in draft form, but it sets out changes that - taken together with developments under the General Data Protection Regulation ('GDPR') - threaten to undermine the business models of many adtech sector companies. This article examines the key issues that the sector will need to grapple with, and considers how these may play out in practice. It concludes with a prediction of three alternative futures, depending on how the final ePrivacy Regulation shakes out:

- one where adtech businesses evolve in the face of tough new cookie rules to rely on device fingerprinting based on signals emitted by user devices;
- one where cookie handling and ad serving are consolidated into the hands of a small number of key players; and
- one where a sophisticated - potentially blockchain based - industry-wide framework is developed that enables cookie powered behavioural targeting on an opt-in consent basis.

To understand why and how these different scenarios may arise, it is important first to look at what the new Regulation proposes, and how this interplays with the GDPR.

Cookies revolution

Lots of different kinds of business may sit within the adtech 'stack,' but many of them rely for their targeting and data enrichment on information derived from cookies posted onto end user devices - or other technologies that may use the processing and/or storage capabilities of those devices. (For simplicity the rest of this article refers just to 'cookies.')

Under the current ePrivacy Directive (Directive 2002/58/EC), cookies rules vary across Member States but generally have been interpreted as permitting a form of 'browse-wrap' consent: pop-up banners put the user on notice of cookies being deployed, with ongoing browsing taken as his/her consent. The new ePrivacy Regulation proposes a dramatic change.

GDPR-grade consent

The draft Regulation expressly imports GDPR standards for consent and applies them in the context of cookie consent. Recent draft ICO guidance suggests this would mean, amongst other things, that valid consent would need each of the following requirements to be met:

- Unbundled: Consent requests must be separate from other terms and conditions. Consent should not be a precondition of signing up to a service unless necessary for that service.
- Active opt-in: Pre-ticked opt-in boxes are invalid - unticked opt-in boxes or similar active opt-in methods must be used (e.g. a binary choice given equal prominence).
- Granular: Granular options to consent must be given separately for different types of processing wherever appropriate.
- Named: The organisation relying on consent must be named - merely stating a category of entities, even if precisely defined, will likely not be acceptable under the GDPR.
- Documented: Records must be kept to demonstrate what the individual has consented to, including what they were told, and when and how they consented.
- Easy to withdraw: People must be told they have the right to withdraw their consent at any time, and how to do this. It must be as easy to withdraw as it was to give consent: simple and effective withdrawal mechanisms must be in place.
- No imbalance in the relationship: Consent will not be freely given if there is imbalance in the relationship between the individual and the controller.

Practical impacts for cookie consent

Pending the new ePrivacy Regulation being finalised and coming into force, it is likely that Recital (173) and Article 95 of the GDPR mean that the current 'implied consent' regime under the ePrivacy Directive will continue to apply, unaffected by GDPR consent requirements. But once the ePrivacy Regulation comes into effect, it looks like adtech businesses may need to get opt-in consent, on a named basis, in order to set or access cookies. But of course many adtech businesses do not have a direct relationship with end users. So how could a consent of that kind be obtained? And are there any ways around the consent requirement?

Routes for getting GDPR-grade consent

One route to consent may be via browser settings. The draft Regulation pushes strongly for consent to be managed more at browser level and less on a site-by-site/publisher-by-publisher basis. If this is carried through to the final legislation, then adtech businesses could seek to use that browser functionality to ask for consent. There is little clarity yet as to how the browser mechanisms may work, including how requests for consent would be presented. Given that some of the browser manufacturers also have 'skin in the game' in the online

advertising sector, it is to be hoped that cookie choices relating to online ad targeting may be presented in a relatively business friendly light - giving the user some background and context as to the consequences of their choices. However, adtech businesses and their trade associations would do well to engage with the browser companies at an early stage to discuss this. Otherwise, adtech companies will need to look at whether they can get consent themselves, via publishers/advertisers and/or via some industry-wide framework.

Going it alone

For many businesses in the sector, getting prior consent directly from individuals would be a tall order. Most will have no direct line of communication with individuals. Getting consent via publishers/website owners may be a more viable option. But for many businesses, the scale of the task of engaging with numerous publishers may seem prohibitive. In the programmatic advertising ecosystem, impressions may become available across inventory owned by a very large number of disparate operators. Those publishers in turn may feel it is challenging, from both an operational and a user experience/design perspective, to gather named opt-in consent for the potentially very large class of adtech intermediaries who may wish to post or access cookies via their sites. Further, each business relying on a consent via that route would need to hold records demonstrating the consent and would need to have in place easily accessible opt-out mechanisms (presumably promoted via the publishers' sites).

Adtech businesses might also be able to get consents via those advertisers who have direct lines of communication with their customers/targets. Just as brands currently collect opt-in consents for email and SMS marketing, so we may see a rise in tick-box permissions for named adtech intermediaries to use cookies for ad targeting. But again, the sheer number of players in the ecosystem may mean this is unattractive as a typical solution.

An industry-wide solution?

Alternatively, will some industry-wide solution emerge - perhaps some evolution of the current youronlinechoices.eu framework? One can see there may be good sense in having a single universal system - perhaps maintaining a distributed blockchain database of consents - that allows individuals to control their consents for all different adtech businesses and activities. This could be promoted by publishers and advertisers, and could also plug into browser-based cookie choice menus. However, if opt-in consent is required then the trick will be to persuade adequate numbers of individuals to give that consent. With the debate over so-called 'cookie walls'/'tracking walls' ongoing, it is as yet unclear whether the final version of the legislation would allow consent to be validly obtained by offering some financial or other incentive.

Possible ways around the consent requirements

If the legislation remains close to its current form, the only realistic way to avoid the need for cookie consent may be to avoid setting or accessing cookies (or otherwise using the processing/storage capabilities of people's devices). Adtech businesses sitting away from the front line of directly posting/accessing information on user devices may be able to avoid the need for consent under Article 8(1) of the ePrivacy Regulation. They may also be able to argue that they can rely on 'legitimate interests' rather than consent as the legal basis for their processing of personal data for GDPR purposes. Recital (47) of the GDPR states that 'the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.' And while the Article 29 Working Party ('WP29') Opinion 06/2014 on legitimate interests is decidedly sniffy about the applicability of legitimate interests for online behavioural targeting under the Data Protection Directive, there would seem to be a good case for arguing that the enhanced transparency and data subject control requirements under the GDPR should lead to a different analysis under the WP29's balancing test.

Other businesses that have historically relied on posting/accessing cookie data may potentially be able to move away from using cookies. If they can base their targeting instead on less intrusive technologies that just use certain information automatically emitted by the user's device, they may be able instead to rely on the alternative regime under Article 8(2). As currently drafted, this provides for a notice based (rather than consent based) regime for the collection of 'information emitted by terminal equipment to enable it to connect to another device and/or to network equipment.' However, opinions from the WP29, the European Data Protection Supervisor and the LIBE and ITRE committees of the European Parliament have all criticised Article 8(2) and have argued for a consent requirement. So at this stage it is not certain that a notice based regime will survive.

What this all means for the adtech sector

If a notice based regime under Article 8(2) were to survive, then some businesses may potentially see it as attractive to move from cookie enabled targeting to use of 'device fingerprinting' technologies that do not access the processing/storage capabilities of user devices. Those technologies may not be as accurate but could be part of an opt-out based solution, with notice potentially delivered via an icon served with ads, as envisaged under Article 8(3), and where processing would need to be justified under 'legitimate interest' grounds. Alternatively, and particularly if the opportunity under Article 8(2) is closed down, we may see large numbers of adtech businesses unable to meet the Regulation's consent standards. Market forces may then lead to consolidation with cookie based targeting and ad-serving operated by just a handful of key players that are able to get valid consents. Other existing businesses may need to evolve so as to work in partnership with those key 'hub' businesses, and avoid setting/accessing cookies themselves. Again, while the hub businesses could rely on consent for their data processing, others may depend on 'legitimate interests' being available (and would need to comply with applicable transparency and opt-out requirements under the GDPR).

Finally, it is still possible that a workable industry-wide solution may emerge in time to allow adtech businesses of all shapes and sizes to get GDPR-grade consent. However the shift to named opt-in consent will likely result in overall consent levels plummeting, which itself may drive further consolidation in the marketplace.

Timescales

The European Commission originally hoped to have the ePrivacy Regulation come into effect at the same time as the GDPR on 25 May 2018. However, with a number of potentially difficult points already having been raised in opinion papers from regulators, European Parliament committees and the European Data Protection Supervisor, that deadline looks in doubt. Indeed, the incoming Estonian Presidency of the Council of the EU is now reported as aiming to finalise the ePrivacy Regulation by the end of 2018 rather than 2017. There may therefore be some stay of execution for the adtech industry, but the existential threat remains. If the sector does not move quickly and decisively, many currently successful businesses risk becoming unviable.