ACCC, opt out opt in and future directions for regulation of adtech and programmatic

briefing notes for *IAB State of Data – Opportunities & Responsibilities* panel on 14 August 2019

The first thing to say is why and how I'm opening this panel discussion and talking to programmatic and adtech people about the ACCC Digital Platforms Inquiry Final Report.

To date most discussion of regulation of adtech in Australia has focussed upon privacy regulation and expectations of the Australian Privacy Commissioner as to online behavioural advertising and disclosures as to uses of online tracking code.

The EU has had a longer running, and quite narrowly focussed, debate about tracking cookie consents and real time bidding practices. The debate has partly been:

- between the adtech and programmatic sector and the regulators;
- between privacy advocates, supply side players (digital platforms and publishers); and
- between the EU member state national regulators, including significant disagreement over what the GDPR actually means and requires, and how changes to the proposed ePrivacy Regulation should further restrict deployment, use and sharing of online tracking code and device identifiers, in particular through cross-device tracking and third party cookie matching.

Continuing uncertainties as to likely regulatory outcomes in the EU have delayed finalisation of the iab Europe's transparency and consent framework for, in particular, use of third party tracking code.

In the last two months, the UK ICO and France's CNIL have upped the pressure on the adtech sector by saying 'no more soft opt-in' and instead signalling that they require that providers obtain "freely given, specific, informed and unambiguous consent" to initial drop and subsequent uses of tracking code or device identifiers that are used to affect whether and how an individual is targeted for marketing. This would effectively require each online marketer to maintain a verifiable evidence trail back to a captured as to what tracking was to occur, and to take active steps to renew a consumer's awareness of what tracking the consumer had previously authorised, such as through regular (six monthly?) reminders. In essence, the UK ICO and France's CNIL gave industry a limited period to address this requirement through industry solutions, or expect regulatory interventions.

Meanwhile, the ACCC has caught up with these more interventionalist and active EU regulators, and now proposes to sprint straight past them. The ACCC proposes an even more interventionist approach, starting from:

- a very high expectation as to the level of transparency and explanation that industry players should provide as to uses of consumer data,

- a proposal to introduce fairness (to consumers) as a relevant touchstone (without any real guide yet to assist industry to work out what is considered unfair and whether useful guidance will be provided to assist industry players in working this out.

How did this happen?

About 18 months ago the ACCC was briefed to report on how operations of global digital platforms were affecting the structure of the news media in Australia and reporting of the news in Australia.

Yet now, and over a 1,000 pages later, the ACCC is promoting fundamental reforms to privacy law and other changes that would cause the programmatic sector to look nothing like it looks today.

How did we get here?

Well, the starting point is to realise that the adtech industry is built on secondary uses of consumer data.

The ACCC is a competition and consumer protection regulator.

It sees its role as to enhance consumer welfare.

The ACCC reviews uses of consumer data through that prism, asking whether consumers are better off, or worse off, through how consumer data is being used in a market.

Sometimes the ACCC in direct aid of consumers, such as by challenging consumer terms as unfair contract terms, or business practices as misleading or deceptive.

More often, the ACCC operates indirectly, through use of competition enforcement powers to challenge misuse of market power, or to improve economic efficiency of markets. For example, in the petroleum retailing sector the ACCC concluded that lack of transparency as to prices enabled some retailers to maintain high prices, so ACCC promoted real-time price comparison services to reduce pricing opacity, even though this arguably also enables coordinated pricing across retailers that reduces competition.

There are many things that the ACCC dislikes, but three things that the Commission really hates.

The first is that most of the Commission's competition and consumer protection powers are only exercisable after-the-event – that is, a power to obtain remedies only after there is a proven breach of the law. The Commission would like more powers to intervene up front, to shape markets and what entities do, and must not do, in those markets before the event.

The second is that the key competition powers of the ACCC require the Commission to prove a "misuse of market power", or a reduction in effective competition, within a "market" as defined in economic terms. This is tricky and expensive work. The Commission often loses complex competition cases and is then ordered to pay a defendant's costs. The Commission would prefer to have, and use, simple powers to determine what it thinks is "unfair" and direct entities accordingly. That is also why the Commission loves its consumer protection powers, as it is simply not necessary to prove any adverse effect upon competition in a market. This is why the Commission is continually agitating to have its consumer protection powers expanded and further simplified, such as by making

it illegal for an entity to propose unfair contract terms in dealings with SMEs or consumers. And expansion of the ACCC's consumer protection powers plays well politically – which Senator wants to say that she or he is against increased protections for consumers? New consumer protection powers are likely to be politically popular, and when enacted give the ACCC a comparatively easy end run on enforcement action against digital platform providers and others. And the ACCC has favoured regulator status with the Australian Treasury (the deepest pockets in government), a relatively good relationship with consumer advocacy organisations, and no great love of digital platforms, advertising and advertisers.

The third thing that the Commission really hates is not really knowing what is going on, upfront: not knowing how a market *really* works. The Commission hates opacity.

The ACCC is not particularly interested in promoting views of privacy advocates.

Some privacy advocates are promoting a view that any secondary uses of customer data to derive inferences about particular individuals (whether or not identifiable) should require prior notice to the affected individual and provision of an option to opt-out of such uses.

This view, if adopted, would preclude many existing uses of customer volunteered or observed (i.e. transactional) data within many businesses, such as uses for scoring and application of customer behavioural factors.

This view if adopted would require provision of an opt-out from many analytics applications.

This view goes much further than current GDPR restrictions on profiling, which only require, in GDPR terms, "unambiguous express [opt-in] consent" when profiling will have significant legal effects upon how an individual is treated.

Privacy advocates do not draw relevant distinctions between secondary uses of data made within an organisation and secondary uses made by third parties such as data analytics services providers.

In each case, the focus is upon what is done (not who does it), whether notice should be given as to what is being done, and the appropriate form of notice/consent as to what is being done.

If publishers adopt either an opt-out or opt-in model, they will likely need to define scope by what is done, rather than who does it. This will likely lead to significant constraints on what they can do themselves, because it will not be practicable to distinguish what they allow themselves to do, and what they say they will not allow others to do.

Transparency as to what is done (and as importantly, what will not be done) by way of controlled and safeguarded secondary uses of customer data could be afforded through more fulsome disclosure in a general privacy policy and in privacy notices for particular products, without any need for provision of either opt-out or opt-in choice functionality.

Clarity, simplicity and prominence in disclosures (transparency) is the key factor in nurturing digital trust, not provision of choice functionality (whether opt-out or opt-in). Many consumer advocates now rightly observe that consumers don't want or need more decisions forced on them: what consumers want is organisations that are data custodians to be open, transparent and acting

responsibly to nurture consumer trust, rather than an organisation 'passing the buck' back to the customer to make a choice that many consumers feel not competent to make.

This new emphasis upon clarity, simplicity and prominence in disclosures, including as to controlled and safeguarded deidentification (anonymisation) based data linkage, is in my view more conducive of customer trust than data custodians fiddling about with choice architecture (opt-in or opt-out).

This new approach is demonstrated by recent changes to privacy policies and notices of entities such as Velocity and Qantas Frequent Flyer, in each case with active regulatory oversight by both the ACCC and the Australian Privacy Commissioner.

Why a debate over programming and adtech feels like a high road to nowhere

Discussion of regulation of adtech is moving from being principally a debate about consent to cookies towards being a much broader discussion about consumer expectations as to how information about their activities is used, and by whom, and as to 'fairness'.

For stakeholders in the programmatic and adtech industry sector, this is a dangerous shift.

As to consumer expectations, initiating a discussion with affected individuals can lead to unpredictable and uncontrollable outcomes. Explanations of many data applications and data value chains can be devilishly tricky, and can sound self-serving, or just plain spooky. Try explaining to sceptical citizens and consumer advocates how real time programmatic advertising does not require any disclosure of the identity of ad recipients, or explaining how audience segmentation value is allocated at points in the advertising and media supply chain. Even tech-savvy listeners often will not understand the complex data ecosystem that enables audience segmentation and programmatic.

As to fairness, there is a huge gap between a requirement that businesses *not do or say things that are misleading or deceive*, and *not do things that are unconscionable*, and a requirement that businesses *be fair*. What is fair, and what is not, is a highly subjective and complex question. This is the principal reason why the law generally does not require businesses to meet a standard of fairness. To work out what is *fair*, it is necessary to assess markets and transactions and to work out what people know (or ought to know), and the unique value exchange underlying different transaction types. A *fairness* discussion also plays into millennial concerns about who is deriving what commercial value from uses of data generated from analysis of their online activities. A *fair sharing of value* discussion is a much harder debate for industry stakeholders than a discussion of *what information is personal information* and *what should a consumer know about uses of personal information about them.*

For example: it may be considered *fair* for my provider of a loyalty card benefits, or my provider of free social networking services, to (after notice to me) collect and use detailed and valuable information about me to enable marketing to me, in exchange for the benefit of provision of without-charge ('free') services to me.

It may be considered *unfair* for an advertiser buying an audience segment that includes me to use a similar level of detailed and valuable information about me to advertise to me, either because I don't derive the same level of benefit, or because I don't understand what is going on.

Or I may be a consumer in a two-sided market that I really don't comprehend, where 'rental' to an advertiser and use by that advertiser of an audience segment that includes (identifiable or unidentifiable) me funds the digital platform provider to provide without-charge ('free') services to me. If that is the case, the transaction may fall within the class of transactions where I am happy to get the third party advertising, because the sale of advertising canvas that is enabled through the digital platform funds me getting a service at no charge. In which case, properly explained to me, I may consider that an activity that initially sounds to me like one sided benefit and *unfair* to me, really is *fair*.

But maybe I'm still worried and think this all sounds spooky because I think that that advertiser gets to know all those things about me that the provider of the digital platform clearly knows about me. To know whether I think the data value exchange is reasonable and proportionate, I need to understand more about the data flows.

Accordingly, the adtech debate often cranks up to another level of complexity, as we start to talk about how the relevant technology works, and what is possible, and what is not, in the management of flows of personal information in the programmatic and adtech data ecosystem.

I'm sorry that this is complicated, but it just is. If a reader knows how to make this simpler and more capable of explanation, I look forward to reading it!

New UK ICO guidance as to real time bidding (RTB)

The EU adtech debate to date has had a relatively narrow focus upon the level of disclosure and the form of affirmative express consent required to be obtained from affected individuals in the EU before drop of cookies or other tracking code.

It has generally been accepted by GDPR regulators and lawyers that online identifiers used to collect data about activities of individuals in the EU are pseudonymised personal identifiers and their deployment and use in relation to individuals in the EU regulated by GDPR.

The most significant issue has been how the existing Cookies Directive[1] (the ePrivacy Directive), and the proposed new ePrivacy Regulation[2], operates together with the GDPR, and in particular as to the circumstances in which an entity can use a third party cookie look-up table (where the party using the look-up table cannot verify that the third party cookie was placed with requisite consent).

Meanwhile in Australia, Singapore and NZ, it has been possible to point to the Australian Privacy Commissioner's comments on adtech[3] and say that properly anonymised and controlled use of online identifiers is not a use of personal information regulated by the Australian Privacy Act.[4]

---

[1] Privacy and Electronic Communications Directive 2002/58/EC on Privacy and Electronic Communications, otherwise known as ePrivacy Directive, as amended by Directive 2009/136.

[2] Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC.

[3] See Office of the Australian Information Commissioner, Privacy fact sheet 4: Online behavioural advertising — know your options, available at https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-4-online-behavioural-advertising-know-your-options

[4] See for example OAIC, De-identification and the Privacy Act, March 2018, at https://www.oaic.gov.au/agencies-and-organisations/guides/de-identification-and-the-privacy-act, and Guide to Data Analytics and the Australian Privacy Principles,

That noted, the Australian Privacy Commissioner has not devoted significant attention to this area for some years, aside from its reviews as to operation of loyalty schemes.

The interim report of the UK ICO on real time bidding (RTB) opens up a broader debate, which more closely aligns with the ACCC's current interest in activities of digital platforms.

The ICO states that:

- The "vast amounts of data" that is used in RTB which builds individuals' profiles is disproportionate, intrusive and unfair. This is especially true given that individuals are often unaware that it is happening.

- Privacy information provided to individuals is overly complex and does not provide individuals with a clear picture of what happens to their data. In particular the ICO notes that organisations must document and be able to demonstrate how their processing operations work, what they do, who they share data with and individuals can exercise their rights. Of course, the nature of RTB with complex data supply chain makes this challenging.

- Processing of personal data in the context of RTB is a "perfect example" of where Data Processing Impact Assessments (DPIAs, or what we in Australian would call a Privacy Impact Assessments (PIAs)), are required under EU GDPR. "In particular, they use new technologies, involve profiling on a large scale, track geolocation or behaviour, include data that is collected indirectly and may involve the use of data about children or other vulnerable groups."

- Market participants seem to be unclear about the rules governing the use of cookies.

- The nature of data sharing within the process of RTB leads to a risk of "data leakage" which the ICO has concluded cannot simply be dealt with by putting contractual controls in place between parties sharing data. The ICO points to the important addition of the accountability principle under the GDPR which requires organisations to demonstrate how they comply with the data protection principles, for example through establishing processes and implementing policies to ensure such contractual standards are satisfied in practice.

On 21 June the IAB Europe published a brief response[5] further promoting the IAB Europe's Content Taxonomy and Transparency and Consent Framework[6] (TCF) as follows:

> The ability to address the ICO's concerns is near impossible to achieve without a standardised industry solution and we share the ICO's aim that parties operating within digital advertising can continue to operate responsibly and in compliance with relevant laws, to ensure the sustainability of this innovative sector which underpins the ad-funded internet.
>
> We also welcome the opportunity to clarify some of the misconceptions in the report's description of the features and functionality of the Transparency & Consent Framework (TCF). The TCF provides a common framework to facilitate compliance with certain of the requirements of the ePrivacy Directive and the GDPR for every part of the advertising value

March 2018, at https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-data-analytics-and-the-australian-privacy-principles

[5] https://www.iabeurope.eu/all-news/press-releases/iab-europe-press-statement-on-uk-icos-adtech-update-report/

[6] https://advertisingconsent.eu

chain, from publishers and technology companies through to agencies and advertisers. In addition, the TCF ensures publishers and advertisers can provide users transparency and choice about the processing of their personal data while continuing to maintain choice in the technology companies with whom they wish to work.

The Content Taxonomy provides nomenclature for categorizing content. It can be applied by publishers and other companies in conjunction with OpenRTB[7] – a communication protocol supporting real-time bidding – and other technologies to allow for better placement of advertising alongside editorial, notably including avoidance of ads for content falling into sensitive categories. Companies choosing to implement the OpenRTB protocol and Content Taxonomy are responsible for ensuring that any personal data they pass or receive complies with the privacy laws and restrictions of their jurisdiction. This is similar to a companies' use of any similar technology, such as HTTP or Wi-Fi.

The ICO's expressed concerns go to the structure of the adtech industry.

The report suggests that the adtech industry should within six months create innovative solutions which embed individuals' privacy in the RTB process, but provides little guidance as to how this can be done in a compliant way.

Note the ICO's emphasis upon fairness, as well as unambiguous express consent. This is where the analogy to what the ACCC are saying, as discussed below, is very clear.

New UK ICO guidance as to use of cookies

Meanwhile, the never-ending EU cookie consent debate rages on.

On 3 July 2019 the UK ICO updated its guidance on the rules that apply to the use of cookies and other similar technologies.[8]

It is now over a decade since EU regulators changed the EU legal requirements for use of cookies and like identifiers from 'notice and opt-out' to 'notice and consent'. That change created challenges for businesses in balancing expectations of regulators, effective functioning of internet services, and providing a reasonable user experience.

As the UK ICO now sees it:

- collection of personal data relating to data subjects in the EU through use of non-essential cookies require unambiguous express consent. Enabling a non-essential cookie without the user taking a positive action before it is set on their device does not represent valid consent. 'Legitimate interests' under EU GDPR will not cut it as a ground for dropping and use non-essential cookies,

- advertising and analytics cookies are not 'strictly necessary' and so do not fall outside the cookie consent rules. While advertising cookies may be seen as crucial by the website or

[7] https://www.iab.com/guidelines/real-time-bidding-rtb-project/

[8] https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/. For useful explanation, se the UK ICO's blog at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/blog-cookies-what-does-good-look-like/.

mobile app operator (by enabling derivation of revenue that funds a service), they are not 'strictly necessary' from the perspective of the user and therefore non-compliant,

- cookies must not be set on landing pages before consent is obtained,
- implied consent therefore will not cut it,
- nor will statements such as 'by continuing to use this website you are agreeing to cookies' do not meet the requirements for valid consent required by the GDPR,
- pre-ticked boxes or any equivalents (such as sliders defaulted to 'on') cannot be used for non-essential cookies,
- users must have control over any non-essential cookies,
- using a banner, pop-up or splash page may highlight prospective use of cookies, but cannot be used to justify setting of non-essential cookies: a user is not by clear and positive action consenting to cookies (as is required to be GDPR 'unambiguous express consent').

The ICO also takes aim at possible workarounds. The ICO expresses the view that consent mechanisms that emphasise that users should 'agree' or 'allow' cookies over 'reject' or 'block' are really non-compliant 'nudge behaviour' which unduly influence users towards the 'accept' option. Also, burying consent controls in a 'more information' section, rather than as part of the initial banner or pop out or other presentation, does not comply because users are not required to make a choice before non-essential cookies are set.

As to third party cookies, the ICO says that the publisher and the cookie provider must work together to ensure notice is provided and valid consent is obtained. The ICO recommends that third parties that want to set cookies or that provide a product that requires the setting of cookies should include a contractual obligation in its agreement with website publishers to ensure that the cookie consent requirements are effectively dealt with.

In relation to organisations operating outside the European Economic Area (the broader 'Europe' to which the EU GDPR applies), the UK ICO states its view that the cookie consent rules in the UK do not specifically apply. However, to the extent the use of cookies and similar technologies involves the processing of personal data relating to data subjects in the EEA, the EU GDPR will apply. So, if a business is based in the Australia and offers online services designed for or targeted to the European market, then that business will need to comply with the GDPR's requirements in respect of the information provided to users.

Peter G Leonard B.Ec.(Hons) LLM (Syd)
Principal, Data Synergies Pty Limited

T +61 411 089 003
pleonard@datasynergies.com.au
www.linkedin.com/in/peleonard/
https://twitter.com/PGLeonard
https://www.business.unsw.edu.au/our-people/peter-leonard