Is the cookie finally crumbling?

As organisations are expected to proactively make advertising cookies compliant, alternative methods emerge. By **Alison Deighton** and **Claire Saunders** of HelloDPO Law.

The ad tech world has, for some time, relied heavily on cookies to drive business, but it is common knowledge that the use of cookies is not without its issues. With regulators cracking down on non-compliant consent mechanisms, cookie consent rates from website users are plummeting. Will new technologies offer a future where the interests of individuals and advertisers are balanced more satisfactorily? A future where we can live in a world free from the tyranny of the cookie pop ups? Or is the situation a little more nuanced than that?

Where did it all start?

According to 'An Empirical Study of Web Cookies'[1] (the Web Cookie Study) cookies were invented in 1994 to enable "state to be maintained between clients and servers". This allowed a website to, for example, recognise a repeat visitor and remember user preferences.

Clearly cookies have come a long way since then. The Web Cookie Study published in 2016 used a web crawler to identify first and third party cookies (first party cookies being those placed by the website you are visiting and third party cookies being placed by another domain). This often occurs where websites add third party elements to their sites (such as plugins and advertising) placed on browsers. On the 100,000 top websites listed on a website ranking service previously available on Alexa.com, over 3.2 million cookies were found, and the Web Cookie Study noted "an alarming prevalence of powerful, insecure cookies". If the search was repeated today, it seems likely that the number would be significantly larger.

The boom in cookie usage

From their early start as tools to keep track of activity on the site being visited, the use of cookies evolved to enable tracking of users from one site to another, creating and building profiles about them and analysing and predicting behaviours based on the information gathered via the cookies. This proved invaluable to advertisers, with third party cookies becoming a fundamental tool in targeted advertising.

The problem with cookies

Whilst now endemic in the ad tech space, the use of cookies, as the reader will be aware, has not been without issues.

The need for GDPR standard consent for the placement of cookies which are not strictly necessary, alongside the proliferation of the use of these cookies led to a (surely) unintended consequence of a barrage of cookie pop-ups which negatively affect user experience, engendering annoyance, confusion and frustration.

Regulatory response

Regulators, including the ICO, have responded by taking action to ensure that individuals are offered a clear choice and easy ability to reject the placement of cookies. In 2023, the ICO and the Competition and Markets Authority (CMA) issued a position paper on choice architecture[2], wherein they examined how choice architecture can lead to data protection, consumer and competition harms. They also reviewed examples of harmful choice architecture, which included some consideration of cookie pop-ups. At one point the Opinion states: "Where the user is presented with an option that allows them to skip more granular settings, then the ICO expects, as a minimum, an equivalent option allowing them to refuse as well (e.g., a 'Reject all' option as well as an 'Accept all'). These must be presented with equal prominence; the user must understand what they mean and must not be nudged towards one over the other."

The ICO followed this up by writing to companies which run many of the most visited sites in the UK about compliance with cookie banner requirements under the Privacy and Electronic Communications Regulations 2003 (PECR) and the UK GDPR. A good response was reported by the ICO, but their enforcement action did not stop there. In January 2024 the ICO indicated in a blog post that they intend to use an AI tool to trawl websites to identify non-compliant cookie mechanisms.[3]

In September 2021, the European Data Protection Board (EDPB) announced the establishment of a cookie banner task force to co-ordinate a response to complaints filed by privacy advocacy group noyb with several supervisory authorities, which it reported on in January 2023[4]. The task force looked at a number of issues, such as the absence of "reject all" buttons on the first layer of the banner, deceptive button colours and contrast, and inaccurately classified strictly necessary cookies.

"Cookie fatigue" has become a recognised term. The previous Government's Data Protection and Digital Information Bill contained a provision entitled "information technology to enable consent to be given, or an objection to be made, automatically" giving powers to the Secretary of State to regulate technology which would allow for such consent/objection. The move was, however, criticised in the House of Lords for lacking substance in terms of how this would work. It will be interesting to see if the new Government picks up this particular baton when it puts forward its new data protection bill. In the EU, the

> The ICO has encouraged those in the advertising industry 'to move to more private alternatives to third party cookies'.

European Commission has adopted an initiative for a voluntary business pledge to simplify the management of cookies although this has reportedly had difficulties in gaining traction.[5]

Industry developments

The factors mentioned above, which give just a flavour of the activity in this area, have surely started to skew the effort vs reward balance for advertisers and have encouraged the development of alternative approaches.

Within the tech industry there have been moves to decrease the reliance on third party cookies with Apple and Firefox taking steps to block third party cookies by default and Google announcing in 2019 its intention to do the same with its 'Privacy Sandbox' project (more on this below). There has also been a proliferation of providers offering "cookieless tracking solutions".

Elsewhere, action by the Irish Data Protection Commission culminated in the decision that Meta could not use legitimate interests or contractual necessity as legal bases for processing personal data for behavioural advertising. Meta is now using a "pay or consent" model in some jurisdictions (broadly, giving the individual the choice of paying a fee for an ad free service or accepting the processing of their personal data for advertising – which can, and often does in the online environment, involve the use of cookies). This model has been met with criticism by the EDPB which has confirmed that "in most cases it will not be possible for large online platforms to comply with the requirements for valid consent if they confront users only with a binary choice between consenting to processing of personal data for behavioural advertising purposes and paying a fee."[6] The model is also facing challenges under the Digital Markets Act and consumer law in the EU.

At the time of writing, we have yet to hear the results of the ICO's call for views on consent or pay mechanisms which it is undertaking as part of its cookie compliance work. The ICO has said that, as a starting point, organisations looking at implementing such a mechanism must consider the power balance between the service provider and users, equivalence (are the paid-for and ad-funded services the same?), whether the fee is appropriate and whether users are given a clear, easy to understand, informed choice[7]. The ICO has also confirmed it is engaging with Meta and expects it to consider data protections raised by the ICO prior to introducing "consent or pay" to the UK.[8]

Despite the potential difficulties, we note this type of model has recently appeared on some newspaper websites.[9]

The Interactive Advertising Bureau has also developed the *Transparency and Consent Framework*[10] which aims to give individuals more control over their personal data and greater transparency in relation to how it is used, but it has faced challenges in terms of data protection compliance of the framework.

Moving beyond cookies?

So, are third party cookies really in decline? If so, the march may have slowed a little with Google's recent announcement about its Privacy Sandbox project.

The project has been beset by delays and on 22 July 2024 Google announced an "updated approach" whereby, instead of deprecating third party cookies, they would introduce a "new experience" in Chrome which would "allow people to make an informed choice that applies across their web browsing".[11] Google currently accounts for over 90% of the search engine market share in the UK[12] and has a substantial share of the browser market (between 54-63% of the desktop market[13] in the UK over the last year) and therefore this change in approach will have significant repercussions for the move away from third party cookies.

The ICO has expressed its disappointment at the change in plans and encouraged those in the advertising industry "to move to more private alternatives to third party cookies - and not to resort to more opaque forms of tracking."[14] The ICO had raised issues in relation to the original Privacy Sandbox approach, as did the CMA who were keen to ensure that the move did not unfairly advantage Google by causing "advertising spend to become even more concentrated on Google's ecosystem at the expense of its competitors."[15]

At the time of writing, details of the mechanism have yet to be revealed, and Google has confirmed it will be engaging with regulators and the industry in relation to the roll out.

Whilst the original Google plan was in motion, there was a pressing need to consider the future beyond the use of third party cookies (including an increase in the usage of first party cookies and consideration of cookieless alternatives), something the ICO reflected upon in its Opinion on data protection and privacy expectations for online advertising proposals in 2021[16]. The ICO urged organisations to be cautious in their development of new technologies, stating that, following phasing out of third party cookies, "new proposals need to be designed with data protection by design and default considerations from the beginning".

In the Opinion, the Commissioner notes that both the UK GDPR and PECR are technology neutral and apply "to any technique that stores information (or accesses information stored) on an individual's device".

The relevant provisions in PECR are detailed in Regulation 6 which states:

1) Subject to paragraph (4), a person shall not store or gain access to information stored in the terminal equipment of a subscriber or user unless the requirements of paragraph (2) are met.
(2) The requirements are that the subscriber or user of that terminal equipment—
   (a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and
   (b) has given his or her consent.

So, even if a tracking technology does not use cookies, if it is storing or gaining access to information stored on the user's device, consent to use it will be needed.

In its guidance on direct marketing[17], the ICO makes it clear that it uses the term cookies to refer to cookies and other, similar technologies, specifically mentioning that technologies to which PECR applies

could include HTML5 local storage, Local Shared Objects, fingerprinting techniques, technologies like scripts, tracking pixels and plugins.

Despite this, there is clearly a danger that these other technologies are being overlooked from a privacy perspective. A study by academics at the Foundation for Research and Technology Hellas at the University of Crete and Telefonica Research[18] (in part) looked at whether the use of cookieless technologies such as first party ID leaking, ID synchronisation and browser fingerprinting is being captured by consent mechanisms. In relation to browser fingerprinting, the study found that 73.5% of the websites which performed fingerprinting, performed it regardless of the user consent action (whether consenting, rejecting or taking no action). Not all websites were in the EU/UK, but sites within these areas were by no means all compliant.

Another paper by Ido Sivan-Sevilla & Patrick T. Parham of the University of Maryland[19] found that "the implementation of cookie-less tracking solutions by the AdTech complex potentially enables greater dynamic visibility on consumers, longer consumer tracking, and the assembling of more sensitive consumer profiles."

Practical considerations

When exploring potential alternatives to the use of cookies, the key to success will be to really understand the technology. This is (another) situation in which privacy professionals and information technology professionals need to work together. There is a strong need for clear and open communication. As privacy professionals we should be asking the questions which allow us to understand exactly how new technologies and cookieless solutions work so that we can identify whether they fall within the scope of tracking technologies under PECR that require prior consent. We also need to identify the information the solution uses, to enable a proper consideration of whether that information is personal data for the purposes of the UK GDPR.

Be wary of advice that a product "does not use cookies" or "does not use personal data". It will be necessary to explore what the provider really means by this to ensure the use of the technology is not captured by the regulations. In terms of assessing whether personal data is being collected, the question of whether data is truly anonymous is one which requires proper consideration and so assertions made by providers should not be taken at face value.

Any new technology will, of course, have to be assessed for compliance in accordance with all the applicable standards, but given there is the potential for new and unfamiliar technologies, there should be a particular focus on transparency. Any activity which falls within the regulations needs to be clearly explained to individuals, adapting our language to ensure we explain how new solutions work and raise awareness of the new technologies. There will also be a need to consider integration with consent management mechanisms to ensure that users are able to choose whether to allow the processing by these new technologies where this is required by the UK GDPR/PECR.

Whilst the immediate demise of third party cookies may not be in sight, familiarising ourselves with developments in this area is essential in order to prepare for changes as and when they happen.

AUTHORS

Alison Deighton is a Director and Co-founder and Claire Saunders is a Professional Support Lawyer at HelloDPO Law Ltd.
Email: alisondeighton@hellodpo.com
clairesaunders@hellodpo.com

REFERENCES

1 Association for Computing Machinery Library - dl.acm.org/doi/10.1145/2872427.2882991
2 www.drcf.org.uk/__data/assets/pdf_file/0024/266226/Harmful-Design-in-Digital-Markets-ICO-CMA-joint-position-paper.pdf
3 ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/01/ico-warns-organisations-to-proactively-make-advertising-cookies-compliant/
4 https://www.edpb.europa.eu/our-work-tools/our-documents/other/report-work-undertaken-cookie-banner-taskforce_en
5 www.euronews.com/next/2024/04/23/commissions-data-cookie-pledge-crumbles
6 www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-082024-valid-consent-context-consent-or_en
7 ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/call-for-views-on-consent-or-pay-business-models/
8 ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/08/ico-statement-on-metas-ad-free-subscription-service/
9 For example *MailOnline* www.dailymail.co.uk/ offers a 'Mail Essential' subscription at £2.70 per month as an alternative to personalised advertising. The *Independent* www.independent.co.uk/ offers a £4 per month ad-free option.
10 iabeurope.eu/transparency-consent-framework/
11 privacysandbox.com/news/privacy-sandbox-update/
12 gs.statcounter.com/search-engine-market-share/all/united-kingdom
13 gs.statcounter.com/browser-market-share/desktop/united-kingdom
14 ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/07/ico-statement-in-response-to-google-announcing-it-will-no-longer-block-third-party-cookies
15 www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser-changes
16 ico.org.uk/media/about-the-ico/documents/4019050/opinion-on-data-protection-and-privacy-expectations-for-online-advertising-proposals.pdf
17 ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies
18 https://arxiv.org/pdf/2102.08779
19 www.ftc.gov/system/files/ftc_gov/pdf/PrivacyCon-2022-Parham-Toward-Greater-Consumer-Surveillance-in-a-Cookie-less-World.pdf

ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

The new government's strategy – a Labour of (digital) love?

A Digital Information and Smart Data Bill has been promised, but no comprehensive AI regulation. **Nicola Fulford** and **Robert Fett** of Hogan Lovells analyse the government's approach.

The UK election on 4 July 2024 brought the new Labour government a substantial working majority and an opportunity to deliver change to the UK's data industries as part of its commitment to "national renewal". But is its commitment to digital slow and steady, or is it showing signs of passion and energy towards the sector? Will it deliver a digital revolution or simply some pragmatic

Continued on p.3

Vendor management in AI: Must-ask questions and crucial clauses

Organisations looking to buy in AI systems should review their vendor due diligence questionnaires and much more, say **Liza Vernygorova** and **Emma Erskine-Fox** of TLT.

We are currently witnessing a boom in the use of Artificial Intelligence (AI), and this is only likely to continue in the coming years. There is no doubt that AI brings huge potential benefits, but it is easy to get distracted by all the issues that AI promises to solve and the temptation to jump in at the deep end is strong.

However, the use of AI comes with challenges, including vendor

Continued on p.5

Issue 135 **SEPTEMBER 2024**

UNITED KINGDOM
report

ISSUE NO 135 **SEPTEMBER 2024**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Nicola Fulford and Robert Fett
Hogan Lovells

Liza Vernygorova and Emma Erskine-Fox
TLT

Ralph O'Brien
Reinbo Consulting

Sofia Carroll
Naomi Korn Associates

Alison Deighton and Claire Saunders
Hello DPO Law Ltd

Lauren Reid and Meaghan McCluskey
The Privacy Pro

Amy Smyth and Kenzie Baldock
Latham and Watkins

PUBLISHED BY
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* United Kingdom Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.
Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2047-1479

comment

Data sharing takes centre stage in government's plans

The government is drafting the Digital Information and Smart Data Bill, as announced in the King's Speech on 17 July. The ambition of the Bill is to "harness the power of data for economic growth". This includes setting up Smart Data schemes and expanding digital verification services to new areas such as moving house and buying age-restricted goods. Many aspects are likely to remain from the previous DPDI Bill. Read an analysis of the government's plans for digital strategy on p.1.

This issue includes some great management advice for the busy DPO. While we do not yet know the details of the new law, the basics are likely to remain the same but with a twist. Whatever the new requirements may be, it is the DPO's job to communicate the organisation's data processing policy and procedures to the rest of the staff, a job that may sometimes seem like an uphill struggle. There are ways of making data protection sound like an enabler, however (p.15).

The GDPR allows data subjects some control over their personal data, but the question of data ownership is not necessarily clear cut if the data also falls under Intellectual Property law (p.10). There are also intellectual property and data protection implications of training generative AI (p.17).

AI issues already land on many DPOs' desks – for example, it is of vital importance to ensure that AI vendors comply with transparency and explainability obligations. Due diligence, and detailed contract negotiations are needed when deploying AI solutions (p.1).

You can also read about an apprenticeship scheme on Data Protection and Information Governance that has been in operation since March 2022. This programme is a great opportunity, for example for recent graduates, and provides organisations with a skilled workforce (p.8).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you wish to contribute to *PL&B UK Report*? Please contact Laura Linkomies, Editor (tel: +44 (0)20 8868 9200 or email: laura.linkomies@privacylaws.com) to discuss your idea, or offer to be interviewed about your organisation's data protection/Freedom of Information work.

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

PL&B's United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to privacy and data protection law issues and tech developments that will affect your compliance and your reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications.

3. Electronic Versions
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments.

6. Back Issues
Access all *PL&B UK Report* back issues.

7. Events Documentation
Access *PL&B* events documentation, except for the Annual International Conferences in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

9. Free place at a *PL&B* event
A free place at a *PL&B* organised event when booked at least 10 days in advance. Excludes the Annual Conference. More than one free place with Multiple and Enterprise subscriptions.

privacylaws.com/reports

"Fantastic documents which provide a useful snapshot of the data protection landscape all in one place that can be easily digested around your busy working day. The split between *International* and *UK* allows you to focus on areas of interest as you require."

Angela Parkin, Group Director of Data Protection, Equiniti

International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 37th year. Comprehensive global news, currently on 180+ countries, legal analysis, management guidance and corporate case studies on privacy and data protection, written by expert contributors

Read in more than 50 countries by regulators, managers, lawyers, and academics.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.