MEDIA LAW INTERNATIONAL ®

e-Zine Q2-23

Research, analysis and opinion on international media law

UK fines TikTok £12.7m for data protection breach

Information Commissioner's Office

The ICO fines TikTok GBP12.7 million for GDPR breaches, including failing to protect children's privacy and unlawful use of data

The Information Commissioner's Office (ICO) issued a fine of GBP12,700,00 to TikTok for breaching UK data protection law.

The fine was issued on 04 April for GDPR breaches that include failure to protect children's privacy and unlawful use of children's personal data.

The ICO investigation found that TikTok "did not do enough" to check who was using its platform and did not take sufficient action to remove those who were underage.

The regulator estimates that the company allowed up to 1.4 million UK children under the age of 13 to use its platform in 2020.

The multi-million-pound fine was initially set at GBP27 million by the ICO.

However, taking into account TikTok's representation, the regulator decided not to pursue an additional breach relating to the platform's unlawful use of "special category data". TikTok welcomed the reduction, adding an investment in internal systems and safeguarding measures. This includes the launch of a safety team of 40,000 employees.

Commenting on the case, John Edwards, UK Information Commissioner, said: "There are laws in place to make sure our children are as safe in the digital world as they are ➔

Twitter approves 83% of requests to restrict content

Twitter has fully complied with 83% of government and court requests to remove or change content, according to a report from Rest of World, a technology publication.

The report was published on 27 April and cites data drawn from Twitter's reports to the Lumen database.

Data shows that between 27 October 2022 and 26 April 2023, Twitter received 971 requestS from governments and courts in the first six months under Elon Musk's ownership. Twitter reported that it fully complied with 808 of requests, which included orders to remove controversial posts.

Following his acquisition of Twitter in October 2022, Mr Musk stated his intention to improve free speech and limit political bias. He explained his reason for acquiring Twitter was to provide "a common digital town square, where a wide range of beliefs can be debated in a healthy manner."

Critics say that Twitter's level of compliance poses a risk to free speech and is in stark contrast with the 50% rate of compliance prior to his ownership.

In an interview with the BBC, Mr Musk commented: "We can't go beyond the laws of a country." He added: "If we have a choice of either our people go to prison or we comply with the laws, we'll comply with the laws."

Data shows that the majority of recent requests were from foreign governments, such as Germany, India, Turkey and the United Arab Emirates, all of which have increased internet regulations in the past year, according to the report. ■

What's inside

Contact
Zineb Serroukh-Ouarda
Managing Editor
zserroukh@medialawinternational.com
+44 7446 525 299

Contributors

CRS CharlesRussell Speechlys

Fortress Investment Group to acquire Vice Media out of bankruptcy in USD350m deal

Fortress Investment Group is set to acquire Vice Media out of bankruptcy following court approval of its USD350 million bid on 22 June.

Online publisher Vice Media filed for bankruptcy on 15 May, just one month after the closure of its flagship Vice News Tonight programme in April.

Amid multiple bids, Fortress Investment Group was reportedly the most "qualified" buyer. Deals involving companies that declare bankruptcy must be approved by a bankruptcy judge, who decides if the buyers plan is "sustainable for the business".

The investor group, led by Fortress, includes Soros Fund Management and Monroe Capital. The group's bid was raised from an initial USD225 million and includes all of Vice Media's assets and some liabilities.

In a statement. co-CEOs Bruce Dixon and Hozefa Lokhandwala commented: "In response to the current market conditions and business realities facing VMG and the broader news and media industry, we are moving forward on some painful but necessary reductions, primarily across our News business,"

Vice Media's assets include Vice News, Motherboard, Refinery29 and Vice TV.

At its peak in 2017, the privately held Vice Media was valued at USD5.7 billion. ■

Denmark finalises agreement for 6% 'streaming tax'

Denmark's Minister of Culture has introduced a 6% tax on streaming services as part of government efforts to "strengthened democratic control of tech giants".

The "cultural levy" was announced on 14 June as part of a broad political agreement on Danish media policy for 2023-2026.

The tax is introduced as a financial culture contribution that is calculated as 6% of the provider's turnover in Denmark arising from the on-demand services.

Revenue derived from the levy will be used to finance the production of local content such as films, fiction series and documentaries. The levy is estimated to generate around EUR20-27 million per year.

The streaming tax only applies to digital streaming platforms and services established in Denmark or other EU Member States.

In a statement, the Minister of Culture, Ane Halsboe-Jørgensen, commented: 'Media consumption in Denmark has changed'.

Ms Halsboe-Jørgensen went on to explain: 'International streaming services are taking up more and more space, and therefore it is absolutely necessary that they contribute to our cultural community. With a cultural contribution of 6%, we ensure that we also in the future have Danish-language films, series and documentaries of high quality.'

Anders Jensen, President and CEO of Viaplay shared his criticism on LinkedIn, stating: 'It will ultimately lead to less investment in Danish TV content and to higher consumer prices.' ■

UK fines TikTok GBP12.7m for GDPR breach

continued from page 1

← in the physical world. TikTok did not abide by those laws.

Mr Edwards added: "As a consequence, an estimated one million under 13s were inappropriately granted access to the platform, with TikTok collecting and using their personal data. That means that their data may have been used to track them and profile them, potentially delivering harmful, inappropriate content at their very next scroll.

"TikTok should have known better. TikTok should have done better. Our £12.7m fine reflects the serious impact their failures may have had. They did not do enough to check who was using their platform or take sufficient action to remove the underage children that were using their platform."

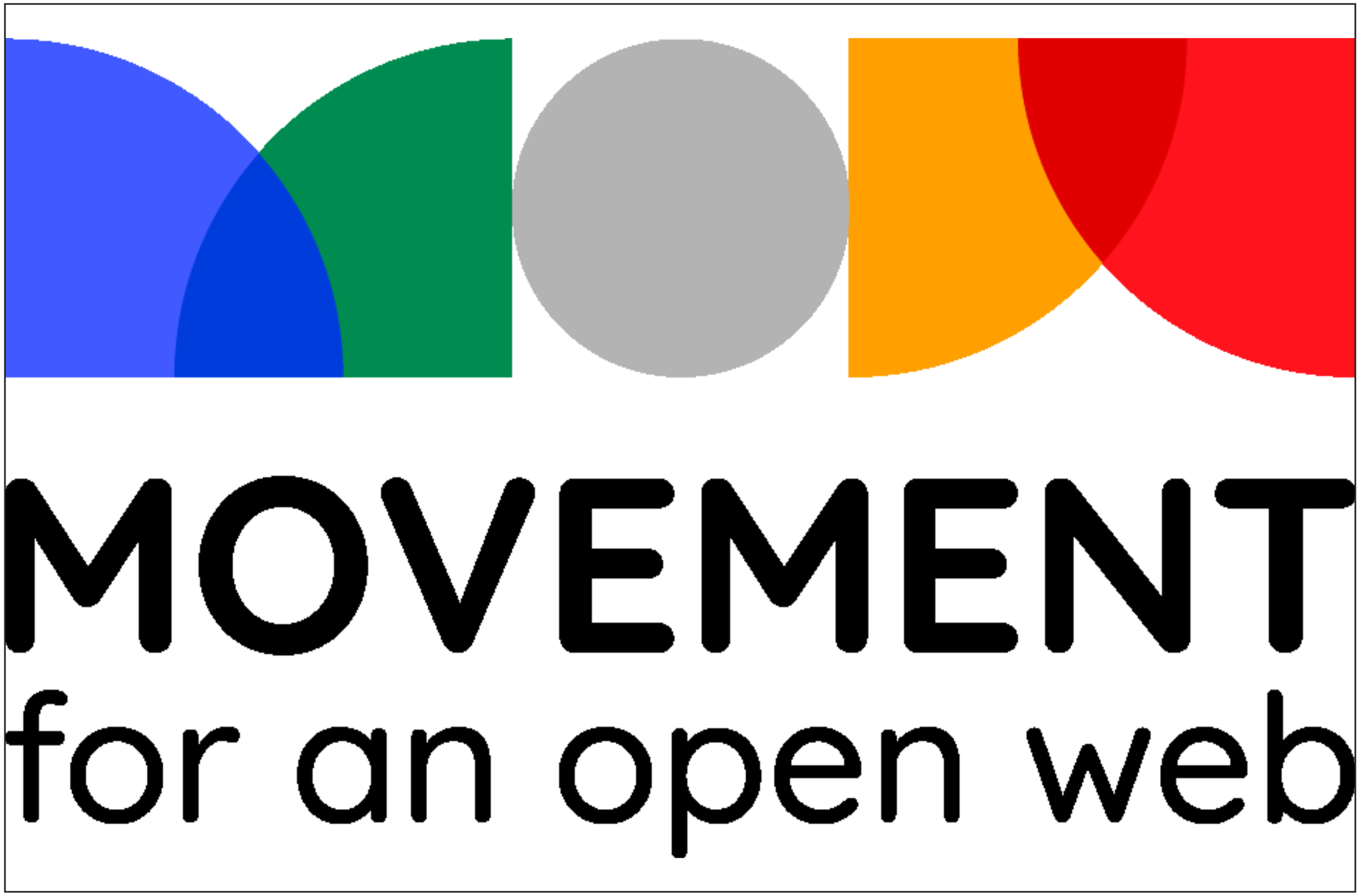
Following its investigation of TikTok, the ICO published the Children's Code to help protect children in the digital world.

The statutory code of practice is aimed at online services, including apps, gaming platforms and social media sites.

Since 25 May 2018, the regulator has had the authority to impose a civil monetary penalty of up to GBP17 million.

Monetary penalties are not held by the ICO but are paid into the Consolidated Fund, the Government's general bank account at the Bank of England. ■

GDPR clarifications offer potential for publisher



James Rosewell, Director of Movement for an Open Web, shares his insight on the topic of digital privacy amid recent precedents

As the EU's General Data Protection (GDPR) celebrates its fifth birthday, it is a good moment to look at the topic of digital privacy following recent precedents which transform our understanding of the law and challenge assumptions. There are real privacy concerns online. Hacking and data breaches are violations of people's private information.

In recent years the privacy debate has moved on from these outright examples of privacy invasion into the area of digital advertising.

Ofcom research from 2022 suggests that 72% of consumers are happy for companies to collect their personal information, including for digital advertising to support free media.

Apple and Google have used supposed consumer concerns about privacy in digital advertising to justify self-preferencing changes that harm publishers. Since consumers aren't as concerned as claimed, the platforms' motivation is somewhat suspect and another motivation may be at work.

The two main online advertising business models: users and usage:

The first party data business model is operated by businesses such as Google and Facebook. They have billions of users. They gather data directly from users' sign-in, search history and every interaction with each of their products. They take this first party data, including very personal data such as emails, and use it to identify what users are interested in. They take data from their first party cookies as well. They build personal profiles. It is a very rich data set.

The law requires users of personal data to get end users' permission for its use. We can call it the "user" business model since it uses user information. It is a very successful business model - both Facebook and Google operate it at enormous scale and now account for 80% of online advertising spend in the UK.

By contrast, independent competing advertisers (the remaining 20%) operate a "usage" business model. As smaller publishers they can't hope to have much direct first party data about users.

Instead, they look at the usage of web browsers and try to divine purchasing intent from usage data. For example, if a user looks for a new bicycle by browsing five different websites, the users' browser must interact with each website.

Chrome or Safari browsers are mainly used. Knowing which browser is visiting each site doesn't help advertisers know which advert to show to which user though.

Cookies can be set by advertisers to match interest with advert. At a simple level they do this by cross correlating numbers in third party cookie files. They add a cookie to a browser.

Each cookie contains a string of numbers and letters: it's like a computer password which is pseudonymised and can be checked and matched by other computers; a match key. This match key doesn't contain personal data. Multiple visits to look at the same thing on different websites can be matched up using the match keys and may indicate buying interest.

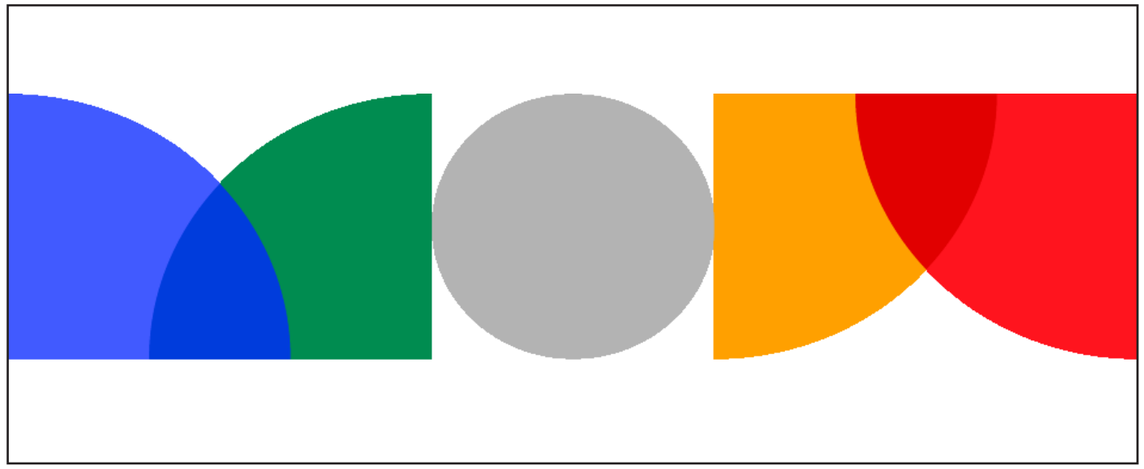
Matching many users' interests in bicycles to adverts for them can then be done very quickly via an advertising auction: bike makers bid in an online auction to advertise their bikes using usage data from many cookies with some confidence that they are promoting adverts that bike buyers are interested in. Importantly for the 20%, usage data from many 3PCs enables them to compete with the scale of Google and Facebook and their user-based business model.

Are first and third party cookies different?

Cookies were created to help computer browsers "talk to" or "interoperate with" websites worldwide. They help maintain continuous computer sessions, so that each visit to a website is quicker and website pages don't have to be reloaded every time a page is turned. They are vital for the operation of the open web.

Adverts for things users don't want tend to be annoying. Cookies also help to limit the number of ads shown, (capping their ➔

GDPR clarifications offer potential for publisher



frequency) and attribute the user click or interest to a successful advertiser. The cookie protocol isn't owned by anyone but has been agreed by the industry as a whole through a central standards making body, in this case the Internet Engineering Task Force (IETF) and technical precedent.

As the CMA noted: "Cookies can be set by first and third parties. The web standards community generally defines a cookie as first party when the registrable domain of the page visited by the user matches the registrable domain of the cookie. If the registrable domains do not match, then the cookie is considered third-party to the page.

To illustrate, facebook.com can set a first-party cookie on a browser that is visiting a webpage on facebook.com, and facebook.com can set a third-party cookie on a browser visiting guardian.co.uk. The first party is the

site the user is visiting, which changes as they browse; thus the same cookie may be first or third party depending on the user's context. There is no technical difference between how first and third-party cookies work intrinsically, although browsers may treat them differently."

Most importantly, advertising identifiers stored in 3PCs by those competing with Google and Facebook don't reveal your name, your credit card number or your sexual preference. They simply identify a browser using pseudonymised match keys to enable websites to interact. It is an automated system for matching up adverts for products with likely interest in them. So far so uncontroversial, you might think?

But in recent years, the cookie has become the hub of a war between the digital giants (Google, Apple, Meta and more) and the wider advertising industry.

The privacy sandbox: Apple and Google have been at the forefront of the demonisation of the 3PC. In 2019, Apple's announced "Intelligent Tracking Prevention" to block the use of third party cookies and followed that up with blocking the use of cookies by third parties in its "Apps Tracking Transparency" initiative.

Similarly, in 2019, Google unveiled a new technology platform for advertising called the 'Privacy Sandbox'. This would, it claimed, enhance people's privacy online by blocking third party cookies and replacing them with a system of Google's own devising.

This would prevent - Google claimed - evil advertising businesses (such as news publishers like the Guardian in the CMA example above) from stealing your personal data by retaining it within Google's trusted walls.

Some - myself included - disagreed. Since advertising cookies don't use personal data the 3PC is not a privacy-harming technology and the real driver behind the introduction of the Privacy Sandbox was, in fact, Google's desire to control even more of the online advertising market.

By removing 3PCs from its Chrome Browser - which makes up 65% of all web usage - Google will prevent competing advertisers and media owners from controlling their own data flows. Instead advertising will be diverted into a closed and proprietary, Google-owned system.

The authorities were asked to intervene. Following a complaint from an organisation I founded,

The Movement for an Open Web (www.movementforanopenweb.com), the UK's Competition and Markets Authority (CMA) agreed with our concerns and imposed a set of conditions on Google.

These restrict its ability to roll out the technology worldwide until it demonstrates that its technology is functionally equivalent to the cookies that it replaces.

This process delayed Google's intended timeline for the blocking of 3PCs and roll out of Privacy Sandbox until it can show that competition is not harmed. But it hasn't made it go away.

In May this year, Google stated that it remained committed to blocking 3PCs from Chrome by the second half of 2024. The core issue is still that Google's new products give Google greater dominance of the online advertising industry based on its user profiling business model while failing to increase consumers' privacy.

First party good, third party bad: The core weakness in Google's argument is that first party data and its user based business is somehow good whilst third party data and usage based business is somehow bad. In their worldview, third parties are nefarious online advertising companies with an insatiable thirst for private data, whilst first party data owners are honest and trustworthy businesses such as Google.

The evidence doesn't back this up. Google has been fined many times for breach of privacy laws. Recently, it was fined nearly USD 400 million in 2022 for privacy breaches. Facebook was just last month hit with a £1 billion fine by the Irish privacy regulator.

It is simply not true that third party cookie data is qualitatively worse than first party cookie data. As described above, an advertising cookie is a pseudonymised piece of information that doesn't in itself connect the information it holds to a known person.

Programmatic advertising operates a usage based business model that doesn't need to know more to successfully serve ads to match purchasing interest. The likes of Google and Facebook, however, collect first party data and build profiles that is far more personal. If, as the fines suggest, the user based businesses have a trust deficit when it comes to privacy, how is their holding truly personal information somehow better than another company holding pseudonymous data?

Article by James Rosewell

Director, Movement for an Open Web

The legal position: The issue about cookies being a vehicle for privacy invasion originally arose when, in 2011, Google set Cookies on Apple's Safari browser: without so much as a "by your leave" or the permission of Apple users.

Some Apple users brought a collective action against Google for invasion of their privacy. In 2021, the UK Supreme Court dismissed the case because there was no evidence before the court that the 3PCs Google had set were taking personal data.

The privacy argument for the removal of the pseudonymised identifiers in cookies has been further weakened by the recent European Court judgement on the case of SRB vs EDPS. This case centred on a supposed data privacy breach by the SRB when it passed survey results to Deloitte.

The identity of the respondents to the survey had been pseudonymised by replacing their names with an alphanumeric code. The SRB argued that, because Deloitte had no legal means to reidentify the individuals with the data they held, the data was not personal data in itself and could not be linked up by Deloitte with other data to identify an individual.

The court agreed, setting an important precedent that pseudonymised data that is not capable of being legally re-identifed by the holder of that data is not personal information.

This tracks directly back to the third party cookie issue. As long as the data transmitted is pseudonymised and it is not possible to reidentify the individual, and agreements between the parties legally prevent such re-identfication, that data cannot be regarded as being "personal data" and no breach of GDPR arises.

Meanwhile, the German Bundeskartellamt's recent report into non-search advertising also emphasised the difference between the user and usage-based business models, and noted that pseudonymised data may not require consent from consumers as it doesn't constitute personal data.

These judgements undermine Google's arguments for the introduction of the Privacy Sandbox. Since 3PCs aren't personal data then there is no privacy benefit to their removal.

The Privacy Sandbox is misnamed and exposed as the naked power grab that it is, a transparent attempt by a monopoly player to block competitors. https://movementforanopenweb.com/

All this means that publishers have a strong case to push back against Apple and Google and regain control and choice over their supply chains and monetisation options. The future does not have to be paying whatever 'taxes' Apple and Google demand.

CRS
CharlesRussell
Speechlys

Market Leading International Law Firm

Guiding you through your most pressing legal challenges and rewarding opportunities

charlesrussellspeechlys.com

London | Cheltenham | Guildford | Bahrain | Doha | Dubai | Geneva | Hong Kong | Luxembourg | Paris | Zurich