Workplace worries
Valuable strategies for dealing with workplace harassment and bullying

More than words
Now is the time for mediation to come into the spotlight and shine

Take a letter
An open letter to the judiciary calls for five specific aspects of reform

gazette
LAW SOCIETY

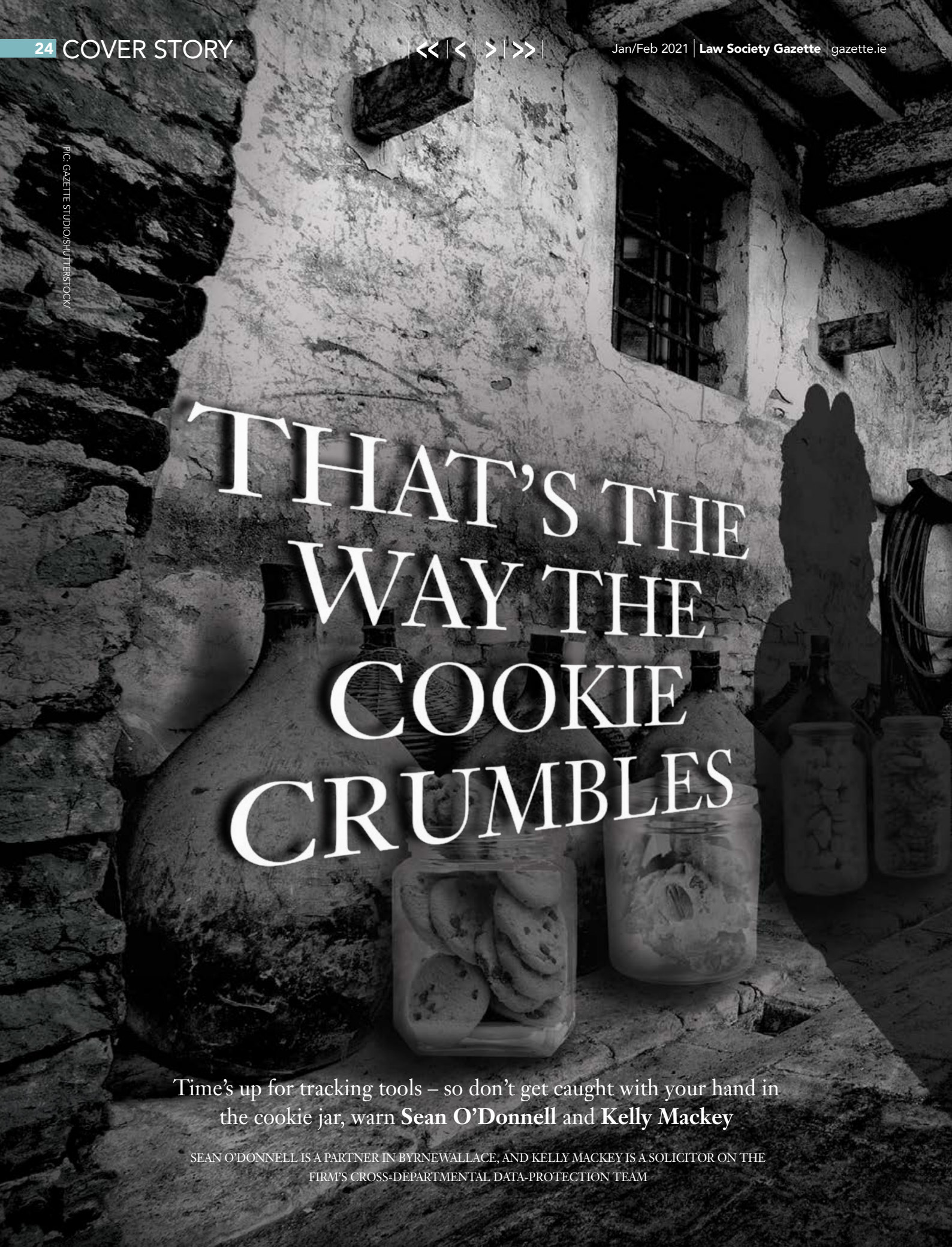
€4.00 **JAN/FEB 2021**

LAW SOCIETY OF IRELAND

CACHE IN THE ATTIC

Are you a cookie monster?

02
9 771393 695029



PIC: GAZETTE STUDIO/SHUTTERSTOCK/

THAT'S THE WAY THE COOKIE CRUMBLES

Time's up for tracking tools – so don't get caught with your hand in the cookie jar, warn **Sean O'Donnell** and **Kelly Mackey**

SEAN O'DONNELL IS A PARTNER IN BYRNEWALLACE, AND KELLY MACKEY IS A SOLICITOR ON THE FIRM'S CROSS-DEPARTMENTAL DATA-PROTECTION TEAM

AT A GLANCE

- Cookies can identify and track users as they browse the net
- The grace period for websites and apps to comply with the law governing the use of cookies and similar tracking technologies expired in October 2020
- The DPC has renewed its focus on cookies compliance
- So what do practitioners and clients need to do to ensure compliance, and what enforcement measures can be expected?

The Data Protection Commission's (DPC) six-month grace period for websites and apps to comply with the law governing the use of cookies and similar tracking technologies expired on 6 October 2020.

The deadline was announced in the DPC's guidance note *Cookies and Other Tracking Technologies*, published on 6 April 2020. The guidance sets out measures that data controllers can take to comply with their consent and transparency obligations, and was produced following a 'cookie sweep' in autumn 2019.

A sample of 38 websites were surveyed in the sweep, representing a range of organisational size and sectors. This included media and publishing, retail, restaurants and food-ordering services, insurance, sport and leisure, and the public sector. Of the 38 organisations surveyed, only two were found to be in substantial compliance.

One-quarter of the websites used pre-ticked boxes for consent to cookies, a practice expressly disavowed by the Court of Justice of the European Union (CJEU) in *Planet49* (C-673/17) in October 2019. Overall, the DPC identified compliance issues in the majority of those examined, due to cookies being deployed without any engagement with the user, classifying cookies as being exempt from consent requirements where this was not the case, and reliance on implied consent.

In March 2020, the DPC stated in its annual report that its renewed focus on compliance in this area emanates from "the pervasive nature and scope of online tracking, and the inextricable links between such cookies and tracking technologies and adtech" (p50).

Chocolate chips

Cookies are small data files stored on the user's device that can identify and track users as they browse the web. They are typically classified according to their purpose (for example, functionality, performance, analytics, social media, etc), duration (for example, expiry at the end of the browsing session, after three months, etc), and origin (that is, first party or third party).

PIC: GAZETTE STUDIO/SHUTTERSTOCK/

> THE DURATION OF ANY COOKIE MUST ALWAYS BE PROPORTIONATE TO ITS PURPOSE. A COOKIE REQUIRED FOR REMEMBERING INFORMATION IN A USER'S ONLINE SHOPPING CART SHOULD NOT HAVE AN INDEFINITE EXPIRY DATE

Cookies are one of a number of device-based tracking technologies. Other examples include local storage objects (LSOs), software development kits (SDKs), pixel trackers or pixel gifs, 'like' and social-sharing buttons, and device fingerprinting technologies.

These tools can serve as short-term memory aids between pages or visits to enhance the user's online experience but, left unchecked, can also be used to build behavioural profiles on users. Many EU supervisory authorities recently scrutinised their use in COVID-19 contact tracing apps.

Ginger nuts

Two pieces of legislation apply to cookies and similar tracking technologies:

- The *ePrivacy Regulations 2011* (SI 336 of 2011), which transpose the *ePrivacy Directive* (2002/58/EC) (as amended), and
- The *General Data Protection Regulation 2016/679* (GDPR) and *Data Protection Act 2018*.

Regulation 5(3) of the *ePrivacy Regulations* specifies that tracking technologies can only be used where the subscriber or user has:

- Given his or her consent to that use, and
- Has been provided with clear and comprehensive information that
  a) Is both prominently displayed and easily accessible, and
  b) Includes, without limitation, the purposes of the processing of the information.

The GDPR and *Data Protection Act* also apply where cookies contain identifiers that may be used to target a specific individual, or where information is derived from tracking technologies that may be used to target or profile individuals (recital 30 and article 4(1) of the GDPR).

On the interplay between the *ePrivacy Directive* and the GDPR, the European Data Protection Board (EDPB) has opined they are intended to coexist and are governed by the principle of *lex specialis derogate legi generali* – special provisions prevail over general rules. In practice, this means that the directive and, by extension, the regulations, serve to particularise and to complement the

provisions of the GDPR in circumstances where both apply (Opinion 5/2019, pp 13-14.)

Hob nobs

The CJEU clarified in *Planet49* that the standard for consent under the *ePrivacy Directive* is that found in the GDPR – that is, website operators wishing to store cookies on a user's device must obtain active, freely given, specific, informed and unambiguous consent, indicated by a statement or clear affirmative action, and such consent must be as easy to withdraw as it was to give (article 4(11) and 7 of the GDPR).

The court further noted that the directive does not distinguish between personal and non-personal data where consent is required and noted its purpose is "to protect the user from interference with his or her private sphere, regardless of whether or not that interference involves personal data". As such, the act of storing or gaining access to information on a user's device by a tracking tool requires GDPR-standard consent, regardless of whether the information involved is personal data.

Chocolate fingers

The guidance reinforces the requirement for the GDPR standard of consent and provides practical direction on how to achieve it when implementing cookie banners or consent management platforms.

Consent must be:

- *Active* – all tick-boxes should be unchecked and all 'radio buttons' and sliders should be set to 'off' by default. Similarly, consent cannot be implied by continuing to scroll through a website, a view which is also the opinion of the EDPB but differs among supervisory authorities across the EU.
- *Informed* – users must be provided with "clear and comprehensive information", which (in *Planet49*) the court held included information on the lifespan of the cookies used and any third parties that can access the user information gleaned by the cookies. If processing involves personal data, then transparency requirements under articles 12-14 of the GDPR apply. The interface used must not 'nudge' the user to accept cookies by giving unequal prominence to the options to 'accept' or 'reject'.
- *Freely given* – use of the website or app cannot be conditional upon the user accepting cookies. This practice is known as a 'cookie wall'. Some supervisory authorities have identified situations where cookie walls may be permissible. While the DPC did not expressly condemn cookie walls in the guidance, the EDPB is opposed to the practice, as it does not present a genuine choice to users (*Guidelines 05/2020 on Consent Under Regulation 2016/679*, paragraph 39.)
- *Granular* – consent must be sought for each purpose (not each cookie) for which cookies are used.
- *Unbundled* – consent cannot be bundled with other items, such as terms and conditions or privacy notices.
- *Refreshed* – consent must be reaffirmed at least once every six months.

Jammy dodgers

There are two exemptions from the requirement to obtain consent and provide clear and comprehensive information under regulation 5(5) of the *ePrivacy Regulations*. These are known as the 'communications' exemption and the 'strictly necessary' exemption.

The communications exemption applies to cookies whose sole purpose is for carrying out the transmission of a communication over a network. The 'strictly necessary' exemption applies to an online service that has been explicitly requested by the user, and the use of the cookie must be restricted to what is strictly necessary to provide that service.

These exemptions are narrowly defined and do not avail many categories of cookies. In its guidance, the DPC clarified that analytics cookies always require consent – a position that differs from that taken by supervisory authorities in France and Germany. An example of strictly necessary cookies could include those that record a user's country or language preference.

Kimberley

In its guidance, the DPC stressed that the duration of any cookie must always be proportionate to its purpose. For instance, a cookie required for remembering information in a user's online shopping cart should not have an indefinite expiry date and should be set to expire once it has served its function or shortly afterwards.

Mikado

In its July 2019 judgment in *FashionID* (C-210/16), the CJEU held that web operators could be joint controllers of any data, such as IP and browser-related data,

> AS COSTLY TO ANY WEBSITE CONTROLLER IS THE RISK OF REPUTATIONAL DAMAGE AND NEGATIVE PUBLICITY. CONTROLLERS THAT DO NOT COMPLY WITH ENFORCEMENT NOTICES FROM THE DPC ARE LIKELY TO FIND IDENTIFYING DETAILS OF THEIR NON-COMPLIANCE PUBLISHED

> THE ACT OF STORING OR GAINING ACCESS TO INFORMATION ON A USER'S DEVICE BY A TRACKING TOOL REQUIRES GDPR-STANDARD CONSENT, REGARDLESS OF WHETHER THE INFORMATION INVOLVED IS PERSONAL DATA

that constitutes personal data gathered on a website and disclosed to third parties whose plugins, buttons, or trackers are hosted on the website. Operators are advised to assess their relationship with all third parties whose assets are used on their website or app.

Coconut cream

Regulation 17(4) of the *ePrivacy Regulations* provides the DPC with the power to issue enforcement notices. The DPC is empowered to pursue summary prosecution of web operators that fail to comply with an enforcement notice, and a successful prosecution can result in a Class A fine (up to €5,000). Where compliance with the regulations is the responsibility of a body corporate then, pursuant to regulation 25, an officer of the organisation may also be prosecuted where an offence has been committed with that officer's consent or connivance or due to neglect on their part. 'Officer' includes a director, secretary, manager or anyone purporting to act in such capacity, and members where they manage the affairs of the corporate entity.

These powers have not been invoked previously in relation to cookies, but the DPC has used this same power to prosecute offences of unsolicited marketing on ten occasions in 2018 and 2019.

Elsewhere in Europe, there are examples of significant fines being issued for cookie infractions. For example, the Spanish supervisory authority fined the airline Vueling €30,000 in October 2019 for failing to provide users with options to accept, reject or withdraw consent to cookies in a granular way. Similarly, the Belgian supervisory authority fined a legal news website €15,000 in December 2019 for insufficient provision of information about cookies and failure to obtain consent for certain non-essential cookies.

Rich tea

If an operator uses any cookies that access users' personal data, the DPC also has recourse to its extensive powers under the *Data Protection Act 2018* and the GDPR in order to enforce compliance. These include inspections, audits, investigations, and requiring the suspension of personal data processing under the act, while non-cooperation with the DPC can be met with a fine of up to 2% of global turnover or €10 million under article 31 of the GDPR.

As costly to any website controller is the risk of reputational damage and negative publicity. Controllers that do not comply with enforcement notices from the DPC are likely to find identifying details of their non-compliance published in the DPC's annual report.

The law concerning cookies and other tracking technologies is not harmonised across the EU, and reform in that regard has been rumbling along for some years. The much-anticipated EU *ePrivacy Regulation* has been the subject of intense lobbying, and it is not yet clear when it will be introduced or what its final text will say – the most recent draft would introduce a 'legitimate interest' ground for using cookies in addition to the consent ground. In its guidance, the DPC warns operators from taking guidance from laws not yet agreed or enacted and underscores that, for now, the *ePrivacy Regulations* remain the touchstone for tracking technologies and cookie compliance in Ireland. g

LOOK IT UP

CASES:

- *FashionID* (C-210/16)
- *Planet49* (C-673/17)

LEGISLATION:

- *Data Protection Act 2018*
- *ePrivacy Directive* (2002/58/EC)
- *European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011* (SI 336 of 2011)
- *General Data Protection Regulation 2016/679*

LITERATURE:

- Data Protection Commission (2020), *Annual Report* (1 January to 31 December 2019)
- Data Protection Commission (2020), *Cookies and Other Tracking Technologies*
- European Data Protection Board, *Guidelines 05/2020 on Consent Under Regulation 2016/679*
- European Data Protection Board, *Opinion 5/2019 on the Interplay between the ePrivacy Directive and the GDPR*