June 2019 • Volume 27 • Number 6

IT Law Today

Europe's law and practice update for specialists in information technology

Editorial

In this issue of *IT Law Today* there is an article on the new copyright directive (790/2019) by Robert Guthrie, John Davidson-Kelly and Jamie Heatly of Osborne Clarke. The directive has been hotly debated and imposes more liability on on-line platforms.

Jaya Bajaj and Katie Gordon Penningtons Manches LLP write about the Online Harms White Paper which was briefly covered in the May 2019 issue of *IT Law Today*. Algorithms are the next topic in an article by Simon Stokes of Blake Morgan LLP where a report is given of a recent case *The Racing Partnership Limited and others v Done Brothers (Cash Betting) Limited and others* [2019] EWHC 1156.

R (on the application of Privacy International) v Investigatory Powers Tribunal and others) [2019] UKSC22 is considered, where the Supreme Court, in a welcome judgment, held that the tribunal can be subject to challenge by way of judicial review.

Cynthia O'Donoghue and Curtis McCluskey of Reed Smith LLP examine the decision of *Green v. Group Ltd and others* [2019] EWHC 954 (Ch). Although the decision is essentially about the duties of administrators as this case related to issues concerning use of personal data it will be of interest to readers. The court rightly held that the experienced administrator in the case could sensibly prioritise creditors' interests rather than having to pursue an expensive investigation to find personal data which Cambridge Analytica group companies might have been able to retrieve but only after a lot of effort which would have involved scarce creditor funds being diverted potentially for the benefit of a potential creditor only whose only "claim" was that he may or may not have had his subject access request not fully answered. The Court said: "Whatever the general view of the mode of operation of the Cambridge Analytica business, Prof. Carroll has yet to establish that his personal data has been unlawfully acquired (he acknowledges that his data does not derive from Facebook) or unlawfully processed; and the present liability of Elections to pay compensation has yet to be determined or quantified. The uncertainties attending establishing these matters are precisely why the relief sought in Prof. Carroll's existing action is "pre-action disclosure" not an award of compensation. But whether my view is correct or not I can understand why the Joint Administrators so characterised it without thereby belittling it: and they have treated the claim entirely correctly pending its adjudication."

The case illustrates the fact that appointing experienced, professional administrators who know their duties well can help ensure the company deals with the administration in a proportionate way with the interests of the majority of creditors being paramount and that for those bringing litigation against a company that then goes into administration it can be hard then to obtain access to the data.

Susan Singleton

IN THIS ISSUE

2 New Copyright Directive Published: How will it Change the EU's Copyright Framework?

4 ICO consults on New Code of Practice for Online Services likely to be Accessed by Children

7 IP in Data and Algorithms – Betting on a Bundle of Rights?

8 UK High Court says No. Administrators are not Controllers

9 GDPR One Year On

10 Rights Group Win Allows Courts to Scrutinize Spy Agencies

ICO fines PPI Claims Company £120,000 for Millions of Nuisance Texts

11 Farrow & Ball Fined for Paying Data Protection Fee Late

12 WhatsApp Potential Data Breach

Auditing Artificial Intelligence

www.singlelaw.com

Singlelaw

New Copyright Directive Published: How will it Change the EU's Copyright Framework?

The new Copyright in the digital single market directive has been officially published, meaning that it came into force on 7 June 2019 (Directive 790/2019). However, Member States have until 7 June 2021 to implement the directive and it is only from that date that its provisions will actually start to apply to works and other subject matter that are protected by copyright.

The Commission had originally hoped that a new copyright directive would be an opportunity to harmonise copyright law across the EU to a much greater extent – at one stage there was even talk about a single copyright title that would cover the whole of the EU, rather than separate copyrights covering individual Member States governed by their own national laws. However, those ambitions had to be scaled back. In the end, the DSM Copyright Directive has ended up a collection of provisions intended to address a number of specific issues.

The most controversial provisions and the ones that have attracted the most attention to date are what are now Article 15 – a new press publication right – and Article 17 – increased obligations on content-sharing platforms if they are to avoid liability for copyright infringing content uploaded by their users (these articles were previously known as Article 11 and 13 respectively before revisions to the article numbers). The DSM Copyright Directive does not just consist of these two articles though and we summarise its various provisions below:

Press publication right: Article 15

The press publication right is intended to give publishers greater leverage to negotiate licensing deals with news aggregators, search engines and other online platforms that link through to their content. Although it has been dubbed a 'link tax', the new right explicitly does not prevent acts of hyperlinking. However, it does cover the reproduction of short extracts from press publications – such as headlines, short snippets of an article or photographs (although not "individual words or very short extracts"). The reproduction of these extracts will generally be required to enable consumers to understand what content is being linked to, so online services that provided links to news articles and other press publication content will in practice need to obtain licenses in the future.

Although larger publishers have been strong advocates for Article 15, there have been concerns from some smaller publishers that their lack of bargaining power means that at best they will be unlikely to negotiate significant licence fees and at worst online platforms and search engines will simply stop linking to their content.

The press publication right does not apply to private or non-commercial uses of press publications – a provision that is intended to ensure that it does not prevent sharing of articles by individual users.

Another important change in the agreed text is that the press publication rights will expire only two years after publication.

Increased liability for platforms: Article 17

Article 17 has seen the most changes to the text through the legislative process. The end result is that under Article 17, established commercial content-sharing platforms will be considered to be performing an act of communication when they provide access to copyright protected works or other protected subject matter (such as sound recordings or broadcasts).

As a consequence, content sharing platforms will be required to enter into licensing arrangements with rightsholders and will otherwise be liable for infringing content on their

platforms unless they have satisfied three cumulative requirements:

- they have made best efforts to enter into a licensing deal;
- they have made best efforts to ensure the unavailability of copyright protected works and other subject matter which have been identified to them by rightsholders; and
- they act quickly to remove copyright protected works and other subject matter when notified of specific content and then make best efforts to prevent future uploads in accordance with point 2) above.

Article 17 provides that new (less than three year old) online platforms with a turnover of less than €10 million will not be obliged to prevent future uploads, but will still need to make best efforts to enter into licensing deals and remove specific infringing content that is notified to them.

The adoption of this Article 17 will be generally seen as a win for rightsholders and a blow to Google – which operates YouTube, the content sharing platform that Article 17 is mostly targeted against. However, the final text could have been worse for Google and it is still difficult to assess how this change of the law will actually impact YouTube's and other online platforms' revenue streams. This will in large part be dependent on how the 'best efforts' requirements are interpreted within national legislation and then by national courts and ultimately the Court of Justice. The Directive also provides for "stakeholder dialogues" to take place during the implementation of the Directive, following which the Commission is to issue guidance on the application of Article 17.

Mandatory text and data mining exceptions – Articles 3 and 4

Articles 3 and 4 require Member States to bring in two exceptions that are intended to make it easier to use analytical tools on third party text and other data to extract useful information without infringing copyright or database rights.

Article 3 provides an exception only to research organisations and cultural heritage institutions for the purposes of scientific research. Article 4 provides an exception for lawfully accessible subject matter that is not limited to such organisations but rightsholders can effectively opt-out of this exception by expressly reserving the right to exploit their subject matter in this way.

Fair remuneration for authors and performers – Articles 18 to 23

The Directive provides that when authors and performers licence or transfer their exclusive rights for the exploitation of their works, they are entitled to receive "appropriate and proportionate remuneration". The Directive allows Member States to decide what mechanisms to use to implement that principle but it does require all Member States to put in place:

- transparency obligations, requiring parties to whom authors and performers have licensed or transferred their rights to provide information on the exploitation of their works including revenues generated and remuneration due;
- a contract adjustment mechanism to allow authors and performers to claim additional remuneration when the revenues received are disproportionally low; and
- a right of revocation where there is a lack of exploitation of the relevant work.

There would appear to be scope for a wide divergence in the implementation of these provisions and stakeholders are likely to be active in lobbying Member States during the implementation process.

Other provisions

The other key provisions of the Directive are:

- a new mandatory exception covering the digital use of works for the sole purpose of illustration for teaching – Article 5;

- a new mandatory exception covering the preservation by cultural heritage institutions of works that are permanently in their collections – Article 6;
- measures that will make it easier for cultural heritage institutions to make available out-of-commerce works that are permanently in their collections – Articles 8-11;
- changes to the EU's collective licensing rules, which allow (but don't require) Member States to give collective management organisations the ability to provide licences for rights of rightholders who have not contracted with the collective management organisations – Article 12;
- a requirement on Member States to establish or designate an impartial body to assist with the negotiation of licensing of audio-visual works on video-on demand platforms – Article 13; and
- a prohibition on non-creative reproductions of works of visual art in the public domain attracting copyright or related rights – Article 14 (this will mean, for example, that a non-creative photograph of the Mona Lisa would not itself attract copyright protection).

Implementation in the UK

Whether the new Directive will ever be implemented in the UK will depend on when and how the UK leaves the EU. The implementation deadline for the Directive is after the expiry of the transition period in the draft Withdrawal Agreement – during which the UK would be required to comply with any implementation deadlines. However, that transition period is extendable and any such extension would therefore require the UK to implement the Directive.

Robert Guthrie, John Davidson-Kelly and Jamie Heatly, Osborne Clarke

ICO consults on New Code of Practice for Online Services likely to be Accessed by Children

Last month IT Law Today mentioned the consultation on online harms. Below the article covers this in more detail:

The Information Commissioner's Office (ICO) has released a draft code of practice for online services that are likely to be accessed by children under the age of 18 (the code).

The code has been issued under the Data Protection Act 2018 and introduces 16 standards of age appropriate design for online services. The code is wide reaching and may apply even if online services are not specifically directed at children.

The focus of the code is having regard to the best interests of children. Non-compliance with the code means online service providers are unlikely to be able to demonstrate compliance with data protection laws, leaving organisations liable to action by the ICO.

The code is currently in draft form and was open for public consultation until 31 May 2019. The final version will need to be approved by Parliament and is expected to come into effect by the end of 2019.

To whom does the code apply?

The code applies to:

- relevant information society services (ISS);
- which are likely to be accessed by children under the age of 18.

Relevant ISS

A relevant ISS (for the purposes of the code) is:

> *any service (normally provided for remuneration), at a distance, by electronic means at the individual request of a recipient of services.*

This will normally involve the sale of products or access to a specific service.

This is a wide definition and will cover applications, websites, social media platforms and content streaming services.

The ISS does not have to be provided for remuneration. Not-for-profit services or those which are funded solely through advertising will also fall within this definition.

Likely to be accessed by children under the age of 18

The focus of the code is whether a service is likely to be accessed by children under 18, making the application of the code extremely wide reaching.

The code applies not only to services specifically directed at children, but also those that appeal to children (including those directed at adults, which in practice attract children).

The ICO recommends that ISS providers conduct market research to demonstrate conclusively whether or not their service is likely to be accessed by children. If you cannot conclusively demonstrate that adults only will access your service, there is a chance it may be accessed by children and therefore the code will apply. For most ISS providers best practice will be to ensure compliance with the code, since the nature of technology and the modern era means most websites, applications, streaming services and social media platforms are easily accessible and therefore likely to be accessed by children.

Does the code apply to me if my organisation is based outside the UK?

The draft code will apply to all ISS providers that are likely to be accessed by children under 18 years old and are based:

- in the UK;
- outside the UK with a branch, office or other establishment in the UK;
- outside the European Economic Area (EEA) which offer services to users in the UK;
- outside the EEA which monitor the behaviour of users in the UK.

Under the GDPR one-stop-shop arrangement, if the ISS provider has a lead supervisory authority other than the ICO and does not have a UK establishment, the code will not apply.

What are the requirements of the draft code?

The code introduces 16 standards of age appropriate design, all of which must be met to demonstrate compliance with data protection laws when processing children's personal data.

The standards expand on the requirements set out in the General Data Protection Regulation (GDPR) by providing specific practical measures and safeguards for children. Further details of each standard can be found in the draft code, but below is a summary.

Best interests of the child

This should be the primary consideration when online services are designed and developed.

Age-appropriate application

The different age ranges and stages of development should be at the heart of how the ISS is designed.

ISS providers should choose whether they apply this standard to:

- all ISS users by default;
- allow adults to opt-out; or
- all children by default.

In practice, the ISS provider will need either to put in place robust age verification mechanisms or apply the same standards to all users by default. The code makes it clear that age-verification mechanisms must be robust and effective. For example, it must not be possible for a child to bypass such a check by merely ticking a box.

Transparency

The privacy information the ISS provides should be concise, prominent and use clear language suited to the age of the child.

This may involve having additional child-friendly information, alongside the more detailed, technical information for adults.

Detrimental use of data

Personal data of children should not be used in ways that would be detrimental to their wellbeing or go against industry codes of practice (eg the CAP guidance on online behavioural advertising), other regulatory provisions or Government advice.

The code recommends keeping up to date with Government advice regarding the welfare of children in the context of digital or online services.

Policies and community standards

ISS providers should uphold their own terms, policies and community standards (including privacy policies, age restriction, behaviour rules and content policies). This means not only adhering to their own published terms and conditions and policies, but also actively upholding and enforcing any community rules or conditions of use set for users.

Default settings

By default, settings for children must be high privacy (unless there is a compelling reason to do otherwise, taking account of a child's best interests).

This means that the personal data of children should only be visible to other users and third parties if the child specifically edits their settings. If a child attempts to change a privacy setting, the ISS should provide appropriate explanations and prompts.

Data minimisation

As with the personal data of those over 18 years old, collection and retention of children's personal data should be kept to a minimum and only for the specific element of the ISS being used at the time.

Data sharing

Personal data of children should not be disclosed to any third parties, unless there is a compelling reason to do so, taking account of the best interests of the child. An example of a compelling reason to share personal data would be for safeguarding purposes.

Geolocation

By default, the geolocation for a child should be switched off (unless a compelling reason to do so can be demonstrated, taking account of the best interests of the child).

When a child's geolocation is active, this must be clearly signposted to the child.

Parental controls

Examples of controls include settings that allow parents and guardians to limit activity or limit the timings of such activity.

The ISS provider should clearly tell children if a parent or guardian has the ability to monitor their online activity.

Profiling

Profiling is the use of personal data to analyse certain aspects or traits, such as behaviour location and personal interests.

All such profiling should be switched off by default for children, unless there is a compelling reason to do so, taking account of the best interests of the child.

Nudge techniques

Children should *not* be encouraged to:

- provide unnecessary personal data;
- take any action which would decrease their level of privacy protection; or
- prolong the use of an ISS at decreased levels of privacy protection.

Nudges towards pro-privacy actions may be relevant, depending on the age of the child.

Connected toys and devices

These must include effective tools to enable compliance with the code. Any ISS providing connected toys and devices will need to ensure that clear information about the product's use of personal information is provided at the point of purchase and prior to device set-up.

Online tools

Children should be provided with easy access to age appropriate and easy to use tools to enable them to exercise their data protection rights and report any concerns they may have.

Data protection impact assessments (DPIAs)

ISS providers should undertake DPIAs specifically to assess the risks to children and to consider how to mitigate any such risks.

Governance and accountability

ISS providers should ensure policies and procedures are in place to demonstrate compliance with their data protection obligations, including data protection training for all staff involved in the design and development of online services likely to be accessed by children.

As with the theme of the draft code, all compelling reasons to act against any of the above standards will need to take into account the best interests of the child. It is likely a valid compelling reason will most likely relate to safeguarding and welfare.

What happens if I do not comply with the code?

Adherence to the standards set out in the code will be a key measure of compliance with data protection laws. ISS providers that do not comply with the code will find it difficult to demonstrate that their processing is fair and complies with the GDPR or Privacy and Electronic Communications Regulations (PECR). The ICO has various powers to take action for a breach of the GDPR or PECR, including any of the following types of action:

- perform audits;
- consider complaints;
- issue warnings;
- issue stop-now orders; and
- issue monetary fines.

Under the GDPR, monetary fines can be up to €20 million or 4% of global annual turnover, whichever is higher.

Further details can be found at: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/age-appropriate-design-a-Code-of-practice-for-online-services/

Jaya Bajaj and Katie Gordon, Penningtons Manches LLP

IP in Data and Algorithms – Betting on a Bundle of Rights?

Data may be the oil of the digital economy but its legal protection is fragmentary and complex. First it is generally understood there is no such thing as "property" in information as such – so for example an electronic database of information cannot be said to be property in the way that the server on which it sits is property.

The law says that you need to distinguish between the information/data itself (in which there is no right of property), the physical medium on which it is recorded (which is tangible property – it can be exclusively "owned" and "possessed") and the intangible intellectual property rights (copyright, database right and rights in confidential information) that may nevertheless still protect the information.

The EU has been thinking about a new legal right that would protect data – a "data producer's right" – but such a right is a long way off. Because of the uncertainty surrounding how the law protects data contracts are often used to deal with the matter even though the legal basis for the protection of the data may be unclear.

A recent case involving horse racing data illustrates some of conundrums around protecting data – *The Racing Partnership Limited and others v Done Brothers (Cash Betting) Limited and others* [2019] EWHC 1156. The case concerned rights to valuable pre-race data

generated at racecourses which was then supplied to bookmakers and others off-course – to betting shops for example.

The "owners" of the data sought to protect their rights in a number of ways – through breach of copyright, breach of database right and breach of confidence and also an overarching claim in conspiracy – the defendants it was alleged had conspired to use unlawful means (based on claims of breach of contract and IP infringement) to injure the data "owners"/claimants.

At trial the claimants/ data "owners" failed in all their claims apart from in relation to breach of confidence – here the court held the pre-race data was commercially valuable and as the claimants had sought to prevent its distribution off-course they were entitled to protect it – even though the information was potentially publicly available.

What is also interesting is that the court rejected any argument that the relevant data was protected by copyright – it was not "original" enough – it was generated by an algorithm by "pure routine work" not involving sufficient skill, labour and judgment to merit copyright protection. As for database right the use made of the data did not amount to database right infringement.

The case illustrates the challenges that can arise in protecting data. The data "owners" here had to make a number of arguments only one of which – breach of confidence – succeeded at trial. Also the fact that the output of an algorithm had no copyright protection is surprising – this may have been due to the simplicity of the algorithm and the simplicity of the output – a "Betting Show" – a single representative price for each horse in race. Also the judge seemed swayed by a much earlier case involving greyhound racing data which had come to a similar conclusion.

The case also involved an analysis of a contract used to assign the IP in the data to the claimants which the defendants alleged was ineffective – the judge however held it was effective – notwithstanding that he had to carry out a detailed analysis of the contract as a whole and its relevant clauses and Schedules to come to this conclusion. This highlights the importance of getting contract drafting right in such cases.

Simon Stokes, Blake Morgan LLP

UK High Court says No. Administrators are not Controllers

The recent case of *Green v. Group Ltd and others* [2019] EWHC 954 (Ch) dealing with Cambridge Analytica's insolvency has clarified the approach that administrators should take when subject access requests are made to the companies over which they are appointed.

A failed administration...

In the aftermath of the notorious data analytics activities of Cambridge Analytica, companies in this group suffered serious financial damage. Administration proceedings were initiated but the administrators were not able to profitably realise the group's business. Unbeknown to the administrators, the Information Commissioner's Office (ICO) had also seized the companies' laptops and servers, which meant the business could not continue to trade. The failed attempts to market the business led the administrators to place the companies into compulsory liquidation and request that they be appointed as liquidators.

A creditor's complaint...

A contingent creditor objected to the appointment of the administrators as subsequent liquidators. Among various objections, the creditor complained that the administrators had breached duties arising under data protection laws. He sought an Enforcement Notice under the Data Protection Act 1998 against two group companies to request that they comply with a subject access request to provide details of his personal data potentially held by the companies.

The creditor also wrote to the administrators requesting copies of the materials and notes of the oral submissions made at the administration hearing. The administrators allowed the creditor's disclosure application, having rejected it initially, and eventually provided the requested documents.

A few data protection questions...

In its assessment of the creditor's objections, the High Court first referred to previous case law, which had established that a *liquidator* is not regarded as a controller in respect of personal data processed by the company. As a general rule, a liquidator acts as a company's agent and, unless the liquidator takes decisions about the processing of the data as a principal rather than an agent, the liquidator cannot be considered a controller.

Here, the administrators decided not to search for the creditor's data through records of 700 terabytes which had been seized by the ICO. The court agreed that this was a decision that the administrators were suited to make. As agents of the company, the scope of their statutory duty was limited and the interests of one creditor had to be balanced against the interests of the general body of creditors.

The court also said that administrators have no general duty to investigate data breaches by the company relating to third parties (such as data subjects). Their duty only extends to investigating breaches of the duty owed by the directors to the company or its creditors.

The court also accepted the administrators' "commercial judgment in an uncertain legal context" not to appeal the Enforcement Notice as the cost of compliance would have been disproportionate. This was because administrators have the right to prioritise recovering assets before addressing claims and distribution issues. There was criticism, though, that the administrators had failed to "appreciate the legal niceties of a novel situation in a developing area of the law".

Comment

This decision is a welcome judicial clarification that administrators (as well as liquidators) are not controllers. What is more, it confirmed that data protection investigations are not for administrators or liquidators to solve – these should remain in the realm of external regulators and be carried out at the public expense. While this is bad news for data subjects seeking information from insolvent companies, liquidation and administration proceedings should only be used for what they are, not as a "free-floating public enquiry into possible unlawful activity implicit in the business model of the insolvent company".

Cynthia O'Donoghue and Curtis McCluskey, Reed Smith LLP

GDPR One Year On

25 May 2019 marked one year since the GDPR came into effect and heralded an avalanche of reflection and introspection from regulators, practitioners and observers. The UK's ICO has published a blog post in honour of the anniversary and a report on the GDPR's first year.

Unsurprisingly, last year saw a significant uptake of individuals exercising their data privacy rights. There was also an increase in data breach reports, with 14,000 received by the ICO in the first eleven months of the GDPR. Of these, only 17.5% required further action from the organisation.

The ICO says that the focus for businesses next year must be on accountability and recruiting DPOs. The ICO's focus will be pressing ahead with its four statutory codes, with consultations on data sharing and direct marketing likely to launch in June.

The CNIL is one of a number of regulators promising further enforcement action as the GDPR beds in, reinforcing the ICO's view that accountability will be key. The European Data Protection Board has published a summary of enforcement actions taken by the EU Supervisory Authorities over the last year. Of the 446 cross-border cases opened by SAs,

205 of these cases have been assigned to a Lead SA under the one stop shop procedure.

The EDPB reports that 144,000 queries and complaints and over 89,000 data breaches have been made under the GDPR. The majority of cases (63%) have now been closed and 37% remain ongoing. The ICO is currently the Lead SA on 93 cases with cross-border implications.

Taylor Wessing

Rights Group Win Allows Courts to Scrutinize Spy Agencies

Privacy campaigners are hailing a major legal victory after the Supreme Court ruled that the intelligence services should not be exempt from oversight by ordinary UK courts. Privacy International (PI) has fought a five-year case with the government, following the Edward Snowden disclosures that UK spies used bulk hacking techniques which may have had an impact on millions of people, according to PI.

The case was initially heard in the Investigatory Powers Tribunal (IPT) – which rules specifically on cases involving the intelligence services. It agreed in principle with the government that it would be acceptable to use a single, broad warrant to hack every mobile phone in a UK city.

PI fought this first in the High Court, but the government argued that IPT rulings were not subject to regular judicial review. Both the High Court and then the Court of Appeal agreed with the government, but the Supreme Court disagreed. Its decision in *R (on the application of Privacy International) (Appellant) v Investigatory Powers Tribunal and others (Respondents)* [2019] UKSC22 effectively means that IPT decisions can be subject to judicial review in the High Court.

PI general counsel, Caroline Wilson Palow, argued the ruling was a "historic victory for the rule of law. Countries around the world are currently grappling with serious questions regarding what power should reside in each branch of government. Today's ruling is a welcome precedent for all of those countries, striking a reasonable balance between executive, legislative and judicial power," she added. "Today's ruling paves the way for Privacy International's challenge to the UK government's use of bulk computer hacking warrants. Our challenge has been delayed for years by the government's persistent attempt to protect the IPT's decisions from scrutiny. We are heartened that our case will now go forward."

ICO fines PPI Claims Company £120,000 for Millions of Nuisance Texts

The ICO has fined a PPI claims management company £120,000 for sending unlawful spam texts about its services. Hall and Hanley Ltd of Devonshire Street North, Manchester were responsible for sending 3,560,211 direct marketing text messages between 1 January 2018 and 26 June 2018 about PPI compensation claims. The ICO launched an investigation after it became aware of a large number of complaints about the company. It found that Hall and Hanley, which had used a third party for this work, but did not have valid consent as required by law.

Steve Eckersley, ICO Director of Investigations, said:

"Companies which are responsible for generating these types of marketing messages should make sure they are operating legally or face a potential fine. Hall and Hanley should have known better. The laws on these types of marketing messages are strict because they can be very intrusive."

Hall and Hanley claimed that consent to send the marketing had been obtained when people subscribed to one of four websites. However Hall and Hanley were named on only two of these websites' privacy policies and people were required to give consent to receive marketing from third parties as a condition of subscribing – which is against the law.

The messages generated a total of 1353 complaints to the 7726 spam reporting service and directly to the ICO. These included:

"I have not consented to these types of messages and it is very concerning and worrying how this company got hold of my mobile number."

"I have not given the company any of my personal information. I have never had any contact with this company. Receiving text messages like this is very concerning as I don't know what other information they have on me, or where they got this information."

Farrow & Ball Fined for Paying Data Protection Fee Late

Farrow & Ball have been fined £4,000 for failing to pay their data protection annual fee on time. The ICO has issued a warning to others to make sure they do pay otherwise sanctions will follow. This year the ICO started to identify organisations which did not pay their fines and also has started issuing trend reports to show which business sectors are worst at paying fees. The ICO runs a "name and shame" list at *https://ico.org.uk/about-the-ico/our-information/penalty-notices-issued-for-non-payment-of-fee/*

Farrow and Ball alleged that a member of staff had been away which is why the fine should not be imposed but, in the very first appeal of a penalty decision of the ICO, the tribunal did not agree that that was a valid excuse. The fine was due.

Farrow and Ball's fee was set at £2900 (as they are a large organisations, whereas the smallest organisations just pay £35 if they pay by direct debit). It is interesting to see what happened in this case – the recipient of the bill was on holiday. The reminder went to the company secretary (presumably the address registered at Companies House) and staff at Farrow and Ball did not appreciate the importance of that letter to the company secretary. "It was not recognised as important internally".

It is vital to make sure staff realise what correspondence must be handled immediately. This will include any court documents such as claim forms which have deadlines and failure to defend means the case is lost and other official papers and demands. Regular staff training should help ensure those who receive and open the post know how to deal with it.

In Farrow and Ball the tribunal noted that the lady concerned had dealt with data protection before GDPR so was well aware of the requirement to pay annual fees. It was not new to her. There was no hearing of the tribunal but there were 50 pages of evidence which were considered. The tribunal looked at similar cases involving pensions regulation and VAT penalties and the definition of what is a "reasonable excuse".

Although no evidence was presented that the person was really on holiday (which is quite surprising as it was the core of the appeal) the Tribunal did not dispute that fact but even so said there should have been measures in place to deal with correspondence coming in when people are away on holiday.

It said that a "reasonable data controller would have systems in place to comply with the regulations and that the Appellant has pointed to no particular difficulty or misfortune which explains its departure from the expected standard of a reasonable data controller."

In terms of the level of the fee Farrow & Ball did not present any evidence of financial hardship so the £4000 stood. Clearly the "dog ate my homework" type excuses will not cut any ice with the ICO.

The full decision is at *http://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i2408/012%20230419%20Decision.pdf.*

The ICO has issued some trend reports in relation to companies fined. These show:

- 103 monetary penalties for non-payment in 2018
- 85 organisations fined £400
- 2 organisations fined £600
- 16 organisations fined £4,000

WhatsApp Potential Data Breach

The UK in conjunction with the Irish Data Protection Commissioner is looking into a security breach involving WhatsApp. There are two agencies dealing with the incident - the National Cyber Security Centre (NCSC) as well as the Irish Data Protection Commission (IDPC) (lead authority for WhatsApp under the EU GDPR). The ICO advises users to check they are using the latest version of WhatsApp as WhatsApp has announced a potential security vulnerability.

Auditing Artificial Intelligence

The ICO is looking at how artificial intelligence can be audited to check for compliance with data laws. The ICO has issued some views on how AI can exacerbate known security risks and make them more difficult to manage. They are asking for views on this topic and give the following examples:

"A recruitment firm decides to use an AI system based on machine learning (ML) to match CVs to job descriptions automatically, rather than through a manual review. The AI system will select the best candidates to be forwarded to potential employers for consideration. To make a recommendation, the AI system will process the job descriptions, personal data provided by the candidates themselves, and data provided by the employers about previous hiring decisions for similar roles."

The ICO emphasises the importance of making sure that all risks in this areas are properly considered.

www.singlelaw.com

ISSN 0969 3297

IT Law Today is published by: Singlelaw, The Ridge, South View Road Pinner HA5 3YD • Tel 020 8866 1934
www.singlelaw.com

Editor: Susan Singleton, Singletons, Solicitors www.singlelaw.com
Production: Frida Fischer • email: fridafischer@hotmail.com
Marketing: Susan Singleton • Tel: 020 8866 1934 or email: susan@singlelaw.com
Publisher: Susan Singleton

Subscription orders and back issues, sales and renewals: Call 020 8866 1934 • email: susan@singlelaw.com
For legal advice and training on IT/ecommerce/internet and data protection law, email susan@singlelaw.com.