ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Collective actions build against Google, BA, Ticketmaster, Equifax

A Group Litigation Order has been issued on British Airways with an extension to claim time, and Equifax faces representative action.
By **Laura Linkomies**.

After a slow start, we are now seeing representative action in the data protection field in the UK. The *Lloyd v Google* case has significant importance for representative action in general as the Court of Appeal recently decided that even if someone has not suffered financial or emotional damage as a result of loss or unauthorised access to their personal data, they can make a claim. Simply losing control of one's personal

Continued on p.3

Take care before you share: The ICO's draft code of practice

Private sector organisations need to pay attention too as the code recommends data sharing agreements to support accountability.
By **Rebecca Cousin** and **Cindy Knott** of Slaughter and May.

In July, the Information Commissioner's Office (ICO) published a draft Data Sharing Code of Practice ("the code"). This is a noteworthy piece of draft guidance as it will have wide-ranging application. In addition, much has changed in the data protection world since the current Data Sharing Code of Practice was published in 2011. Now is therefore a good time for organisations to review their approach to data sharing.

Continued on p.5

Future PL&B Events

- *Balancing privacy with biometric techniques used in a commercial context*, 29 January 2020, Macquarie Group, London. Speakers include Onfido on its use of biometric data and its experience of the ICO's sandbox.
- *Germany's data protection law: Trends, opportunities and conflicts,* March 2020, Covington & Burling, London
- *PL&B's 33rd Annual International Conference*, St. John's College, Cambridge 29 June to 1 July 2020.

privacylaws.com

Issue 106 **NOVEMBER 2019**

UNITED KINGDOM
report

ISSUE NO 106 **NOVEMBER 2019**

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
Rebecca Cousin and Cindy Knott
Slaughter and May

Aaminah Khan
Barrister, St John's Buildings

Robert Waixel
Anglia Ruskin University

Simon Airey and Jack Thorne
Paul Hastings

Merrill Dresner
PL&B Assistant Editor

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

The UK, the EU and Brexit – once again

With the general election hopefully producing an end to the Brexit deadlock one way or another, several questions remain open for the future of the UK data protection framework. As the Court of Justice of the European Union (CJEU) keeps issuing data protection decisions that are affecting practitioners' life on a daily basis, what about the future? If the UK actually leaves the EU, and is therefore no longer subject to these rulings, what will be the status of the previous rulings of the CJEU in the UK courts after exit?

If the UK leaves the EU without a Withdrawal Agreement, i.e. it has not been ratified by January 2020 and the UK has not asked/been given an extension, a no-deal Brexit would mean that organisations would need to revert to alternative arrangements for international data transfers. The DCMS is starting to prepare its own adequacy assessments – perhaps in vain in the middle of all the uncertainty (p.14).

Facial recognition has caused a stir not just in the UK but around the world. Whilst the ICO has alerted organisations to rules of fair play, France's regulator has ordered two high schools to end their facial recognition programs, and in Sweden, the DPA has imposed a fine of 200,000 Swedish Krona (£16,000) on a municipality that used facial recognition in a school (p.8)

The international conference of data protection authorities tackles these types of questions together. We were pleased to attend the conference in October in Albania, where the ICO was at centre stage as the conference Chair (p.11). We made many new contacts, as the international privacy scene is expanding rapidly with new delegates from Africa and Asia.

The decision to allow *Lloyd v Google* to proceed as a class action will have important consequences for group litigation in the UK. On 4 October, the High Court granted permission for British Airways customers to bring a group litigation order (p.1). The 2018 British Airways data breach occurred under the GDPR so we await to see whether the ICO's intention to fine the company £183,390 million will stick.

In the meantime, the ICO is consulting both on data sharing (p.1) and its aim to seize assets under the Proceeds of Crime Act 2002 (p.7).

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.

Actions ... from p.1

information is sufficient grounds.

The Google case goes back to 2011-2012 and the use of cookies on Apple's Safari web browser to collect personal information on the users. This data included financial details but also information about health, race, ethnicity, and sexuality. Google may appeal to the Supreme Court.

Speaking about the case, Managing Director, Kingsley Hayes, at Hayes Connor Solicitors said: "This is a very significant development which recognises that personal information has a value and when that private data is compromised, the individual has a right to compensation whether or not they have suffered actual, or potential, financial loss or psychological injury."

"The ruling rightly adds further weight and consequence to any breach of personal data, even if a breach only involves an individual's email address. This is likely to open the floodgates as consumers become increasingly proactive about protecting their privacy rights and seeking legal redress. Businesses who are not already taking their data protection obligations seriously will have to step up their data protection practices or face legal action and hefty costs."

"The development is fair and right providing robust clarity that the law sits firmly behind the rights of individuals to have full control of all their personal information and how, when and where this is stored, processed or shared."

Since then, we have seen progress with other cases too – the British Airways case was heard at the High Court on 4 October, confirming the extension of time to make claims. Hayes Connor Solicitors is taking representative action against Equifax, and has launched multi-claimant action against Ticketmaster, with 15 test cases. Hayes told *PL&B* in an interview that the Google case gave them a lot of confidence to proceed.

Ticketmaster case

Ticketmaster customers who bought, or attempted to buy, tickets between February and June 23 this year may have had their data stolen, as well as international customers who purchased, or tried to purchase, tickets between September 2017 and June 23, 2018.

The data hack involved both personal and payment information which could be used to carry out data theft and financial fraud. The data stolen includes names, addresses, email addresses, phone numbers, payment details and Ticketmaster login details. Ticketmaster has admitted that it was hacked by "malicious software" on third-party customer support product Inbenta Technologies.

The ICO investigation on Equifax was carried out under the Data Protection Act 1998 rather than the current General Data Protection Regulation (GDPR), and it was fined the maximum £500,000 fine.

> "The next hearing in the Ticketmaster case is 24 February. We are representing 800 out of the 40,000 potential claimants."

Originally, Hayes Connor offered an out of court settlement for Ticketmaster, but it was declined. On 4 October, the law firm issued one representative action on behalf of an individual. In representative actions, one solicitor will represent all clients and Hayes Connor has now been appointed as the representative in this case. "The next hearing in the Ticketmaster case is 24 February. We are representing 800 out of the 40,000 potential claimants," Hayes said. Currently there are no claimants from outside the UK but if they bought tickets on the UK site and reside in another EU country, they can join the claim.

"We are now waiting to see the ICO's technical report on this case. On 8 November, we received a defence from Inbenta, but I do not expect this case to be resolved until 2020-21," Hayes said.

He explained that different categories of loss have been established, with estimated compensation around £1,500-£3,500, depending on whether the claimant has suffered from fraudulent activity. Claims can also be made for psychological distress. This would involve providing a report from a psychologist showing that a medical condition had resulted. On the other hand, anxiety could be proven by a witness statement.

Hayes Connor have instructed Louis Browne QC and Ian Whitehurst of Exchange Chambers Liverpool in the Equifax, Ticketmaster and British Airways cases. The legal costs in the Equifax case have so far been £500,000 and are expected to rise to £5 million. Hays is very confident about the case. There is no litigation funding in place – the firm acts on a no-win-no-fee basis. Hayes Connor won't charge a "success fee" in this case – typically capped at 25% of compensation received – but expects Equifax will to have to bear the costs.

All the clients are insured, however. In most cases, the loser has to pay the winner's costs and disbursements (other legal expenses such as court fees). This insurance is called "After the Event" insurance (ATE). With ATE insurance, if individuals

AVAILABLE CLASS ACTION PROCEDURES

Under the Civil Procedure Rules, two different types of action are possible; representative action or group litigation orders.

The GDPR enables representative bodies to start a **representative action** on behalf of data subjects even without their mandate. This option has not been included in the UK 2018 DP Act, but the government has promised to review the opt-in requirement in 2020.

A **group litigation order** (GLO) is used to manage multi-party claims when individuals have a common complaint. This method was used in the case of blacklisted construction workers against The Consulting Association (the case was settled). GLO is an "opt-in" regime, which means that individual claimants are not included in the action unless they take positive steps to join.

For now, law firms are not always funding these cases so we are seeing specific litigation funders step in.

lose a group action case, any costs will be paid by the insurance provider.

BA case: only 1% join so far

Legal action will now follow for the breach in which 500,000 British Airways customers' personal data was compromised. Mr Justice Warby ruled that victims have 15 months to join the class action.

In an unprecedented move, British Airways applied to launch its own class action for victims and tried to dictate the claim window, say Your Lawyers, Chesterfield-based solicitors. "Your Lawyers warned that this meant that many claimants – potentially hundreds of thousands – could miss out on compensation, unless British Airways could guarantee that all its affected customers would be notified about the Group Litigation. The airline initially tried to defend the move of a short cut-off period but is now set to drastically change its position."

It is understood that only around 7,500 potential victims contacted lawyers for compensation claims. Aman Johal, Director at Your Lawyers told *PL&B* that this is a little over 1% of the number that could be entitled to claim.

"We're a law firm that has been approached by people affected by the breach seeking legal representation. We are bringing a claim in contract, breach of DP Act 1998 and GDPR, and breach of privacy and breach of confidentiality."

The firm advises individuals to join the Litigation Management Agreement (LMA) to appoint a committee to represent them in the litigation. The creation of a committee is necessary and routine in group litigation of this kind, the firm says. All Your Lawyers' Claimants need to be grouped together to be able to make decisions effectively, to obtain insurance against adverse costs and to agree funding for the costs of disbursements (such as Barristers, Expert Witnesses and Third Party Assistance), Your Lawyers say.

"A group litigation order (GLO) was formed in the October hearing by order of Mr Justice Warby. We have been cooperating with other firms' pre-action in any event, and we complied with our duty to engage in inter-firm correspondence / cooperation as we established the Steering Committee with SPG [law firm] as Lead Solicitor, and us on the Steering Committee," Aman Johal told *PL&B*.

The GLO application was recently heard on 4 October. There is now a court cut-off date set for January 2021. It's too early to tell when a trial window would be for a final hearing, if the action proceeds to that point at all, Johal said.

The Information Commissioner's Office has provided a notice of intent to fine BA a record £183m for the breach. The penalty was the first imposed after the EU's General Data Protection Regulation law was introduced.

What are the common issues in the BA case?

Liability and whether there is an entitlement to compensation are the most common issues. There are also two categories of claimant:

- those affected by the September 2018 hack, and
- those affected by the earlier (but later discovered) reward card hack that took place between April and July 2018.

In terms of compensation per individual claimant, Your Lawyers estimates average damages per claimant at £6,000. "However, for higher level awards where a psychological injury is severe, pay-outs could go up to £16,000. If all of the half-a-million affected claimants were to secure the average claim for damages, this would result in a £3 billion payout."

Damages would be based on the individual merits of cases. "Generally speaking, the more a claimant suffers, the more they may receive. Further, those who have suffered financial losses will also need to factor such losses into their case as well and prove that those losses were a direct result of the data breach."

"Damage" is defined as either material or non-material loss and therefore a person is able to claim compensation if they have suffered non-material loss such as distress or a loss of control over the information, Johal said.

If individuals can claim for distress, the claim is calculated in a similar fashion to personal injury claims in that it is on the claimant to demonstrate that they have suffered distress, and the court would assess the distress based upon the level and length of time the person has suffered.

Anya Proops QC, representing BA, is reported to have said that the ICO's intention to fine the airline had put the company under "enormous pressure" and delayed its response to the claimants.

Mr Justice Warby ruled that BA does not have to notify claimants about the group litigation order via its website or by email. The claimant firms can advertise the group litigation order on their websites or social media. It will also be published on the court's website.

Survey launched on cyber security breaches

The government's annual survey detailing the costs and impacts of cyber breaches and attacks on organisations is being conducted from October 2019 to February 2020.

Businesses across the UK have been selected at random from the government's Inter-Departmental Business Register. Charities have been selected from the Charity Commission database in England and Wales, the Office of the Scottish Charity Regulator, and the Charity Commission for Northern Ireland. Education institutions have been selected from the Get Information About Schools database.

During this period some organisations will be called by an Ipsos MORI interviewer inviting them to take part.

• *www.gov.uk/government/publications/cyber-security-breaches-survey*

Data sharing ... from p.1

Whilst much of the code contains helpful guidance, it is likely to be challenging to follow in its current form in all circumstances. A number of organisations, including the City of London Law Society, submitted comments to the ICO during the consultation period for the code, which closed on 9 September. It is hoped that these comments will be taken into account by the ICO to make the final version of the code as useful as possible.

Background on the code

The ICO is required to prepare the code under s.121 of the Data Protection Act 2018 (DP Act). The code must contain practical guidance in relation to the sharing of personal data in accordance with the requirements of data protection legislation and such other guidance as the ICO considers appropriate to promote good practice.

The code will be admissible in legal proceedings and the DP Act obliges a court or tribunal to take account of it, if it appears to be relevant to the question before them. The Information Commissioner is similarly required to take account of the code when exercising her functions under data protection law. In light of this, it would be helpful for organisations if the code could distinguish more clearly between guidance that explains the legal requirements and optional good practice recommendations that, as the ICO state, "aim to help [you] adopt an effective approach to data protection compliance".

Structure of the code

The code is significantly longer and more wide-ranging than its predecessor. For example, it includes new sections on accountability, data sharing and children, data ethics and data trusts. The code contains more examples and case studies, and also contemplates the inclusion of checklists and template forms, which the ICO plans to add to the final version.

Key points of interest: The code contains a significant amount of useful and welcome guidance. Conscientious organisations that were already complying with best practice will find it easier to follow than others who are still grappling with general compliance issues, but even then, in some circumstances, the code's guidance may be impractical. For example, if the code stays in its current form, data sharing agreements in respect of even the most innocuous data sharing would appear to need lengthy documents with detailed explanations embedded within. As a whole, the code is also currently very focussed on the public sector which may be disappointing to a number of private sector organisations. Some of these concerns, and other key points of interest about the code, are considered below.

Nature of data sharing: The ICO recognises that data sharing can include routine and scheduled data sharing as well as on an urgent one-off basis, but there is little mention of data sharing that falls somewhere in between the two. For example, in the context of private sector commercial transactions, data may be shared once or a few times, but not necessarily as a matter of urgency. In addition, the majority of case studies and examples relate to the public sector. Some organisations may interpret this to mean that the code is less relevant to them, but this would be a mistake as the majority of the code is relevant to all data sharing.

If the code stays in its current form, data sharing agreements in respect of even the most innocuous data sharing would appear to need lengthy documents.

Data sharing agreements: Unsurprisingly, the ICO recommends that as a matter of good practice, businesses sharing data should put in place a data sharing agreement. Not only will this help them with their accountability obligations under the GDPR, it will also help all parties be clear about their respective roles, set out the purposes of the data sharing, cover what is happening to the data at each stage and set standards.

The code states that a data sharing agreement should include provisions to deal with various practical problems that may arise when sharing data, such as:

- being clear about which datasets the parties can share to prevent irrelevant or excessive information being disclosed;
- provisions on accuracy of shared data, for example by requiring a periodic sampling exercise;
- mandating compatible datasets and recording data in the same way;
- setting common rules for the retention and deletion of shared data and procedures for dealing with cases where different statutory or professional retention or deletion rules apply;
- common technical and organisational security arrangements, including the transmission of the data and procedures for dealing with any breach of the agreement;
- procedures for dealing with access requests, complaints or queries;
- timescales for assessing the ongoing effectiveness of the arrangements; and
- procedures for dealing with the termination of the data sharing initiative, including the deletion of shared data or its return to the organisation that supplied it originally.

Until the ICO produces a comprehensive checklist in its final version, this is likely to be a useful starting point for some of the provisions that should be included in a data sharing agreement, albeit not all will be appropriate in all circumstances.

In addition, the code sets out some further provisions that the ICO would expect to see in data sharing agreements. These include:

- an explanation of why the data sharing initiative is necessary;
- the specific aims of the parties;
- the benefits the parties hope to bring to individuals or to society more widely by such data sharing;
- extracts of relevant legislation; and
- a clear explanation of the lawful basis.

It will undoubtedly help organisations to meet their accountability obligations if much of this analysis is agreed between the parties and documented clearly. However, it is not as

obvious that a data sharing agreement is the most appropriate place for this analysis to be recorded. Other suitable logs for this could include data protection impact assessments, records of processing and/or legitimate interest assessments.

Joint controllership

The code briefly mentions joint controllership and the requirements of Article 26 of the GDPR for joint controllers to put in place a "transparent arrangement" (which can be met by way of a data sharing agreement). However, it isn't entirely clear how such an arrangement would then differ from an agreement between independent controllers. The code appears to require this in respect of all controller-to-controller data sharing, whether or not Article 26 applies. In addition, parts of the draft code seem to imply that data sharing renders the participants joint controllers (e.g. where it states that it is good practice to provide a single point of contact for individuals rather than making multiple requests to several organisations with which their personal data has been shared). We suspect this is unintentional and, given the ongoing confusion about when a joint controllership may arise following the recent decision in the Fashion ID case (Case C-40/17)[1], hopefully this will be clarified in the final version [the case deals mainly with the issue of "joint controllership" between Facebook and website operators using Facebook's "Like" button].

Liability issues: One area of uncertainty that organisations often grapple with is around the interaction between Article 82 of the GDPR and the limits on liability agreed between parties in a data sharing agreement. Article 82 provides individuals with the right to compensation for damage suffered as a result of a breach of the GDPR. It also allows a controller to claim back from another controller the part of the compensation corresponding to that other controller's responsibility for the damage. Most organisations currently take the view that any contractual limitations (such as liability caps) agreed between parties, including between controllers, would restrict what could be claimed under Article 82 and it would be helpful if the ICO were to acknowledge this in its final version.

M&A and due diligence: The ICO confirms that the code applies to data sharing in the context of Mergers and Acquisitions (M&A). However, the M&A section is very generic and does not explore in any detail the privacy concerns that will likely come up at different stages of an M&A transaction (e.g. due diligence, integration planning, completion). The M&A section is also slightly confused as it mixes up concepts from share and asset sales and so does not provide practical guidance on the areas it does refer to. This lack of clear guidance on some routine challenges that arise in an M&A context can hopefully be rectified in the final version.

The section on sharing personal data in database lists, however, includes a useful checklist of due diligence questions that an organisation receiving data should ask of its counterparty. Although this section appears to be aimed at certain types of data sharing (e.g. sharing by data brokers, marketing agencies, credit reference agencies, clubs and societies and political parties) rather than M&A, the questions are also likely to be relevant in the context of a business acquisition where the assets being bought include personal data, such as a customer database.

The code states that organisations receiving a database of personal data should make appropriate enquiries and checks, including:

1. Confirming the source of the data;
2. Identifying the lawful basis on which it was obtained;
3. Checking what individuals were told at the time (including reviewing any privacy notices);
4. Verifying details of how and when the data was initially collected;
5. Checking the records of consent, if relevant;
6. Checking that the data is accurate and up to date; and
7. Ensuring that the data received is not excessive or irrelevant.

Data sharing in a litigious context: It is interesting that the code is silent on certain types of sharing such as in the context of disputes, regulatory investigations and litigation. Some of the code's recommendations will be impractical in these contexts. For example, a regulator is unlikely to agree to enter into a data sharing agreement with a company involved in an investigation. It would be helpful if the ICO were to acknowledge this in the code.

Data ethics: The code includes a new section on data ethics which provides guidance on the ethical principles that should be considered when deciding whether to share data, in addition to lawfulness and the technical requirements of data sharing. This could be read as imposing an additional layer of obligation on businesses and would also create uncertainty, as general principles around the ethical use of data are still in development. Having said that, it is likely that a number of the factors the ICO raise in relation to data ethics would be relevant to any general assessment of fairness that a business has to carry out under the GDPR and so should certainly not be dismissed as irrelevant.

Next steps

The final version of the code must be submitted to the Secretary of State and then laid before Parliament for approval within 40 days. The ICO hasn't indicated a deadline for when it will be ready to submit the final version to the Secretary State, but it is hoped that this will happen before the end of the year or early 2020.

For businesses, despite the fact that this is only a draft code, the direction of travel is clear and not entirely unexpected. This code builds on a number of recommendations that were included in the 2011 guidance and that businesses should already have been following. For example, it is difficult to see how businesses can avoid having to put in place data sharing agreements in today's post-GDPR world, nor why they would wish to, given how far they can go to help meet general compliance and accountability obligations under the GDPR, as well as to allocate liability and hence mitigate risk.

Organisations should consider taking the following steps now, to the extent they haven't already:

1. Mapping external and internal data flows to understand where data sharing occurs (as opposed to where data processors are engaged) and why. This applies both to data sharing within a corporate group structure or with third parties;
2. Assessing the implications of the

Fashion ID case and determining which instances of data sharing may amount to joint controllership;
3. Identifying where data sharing agreements should be entered into and on what terms; and
4. Commencing a high-level review of existing data sharing agreements. Whilst the final version of the code will provide more definitive and additional guidance (including a checklist of provisions), it should still be possible to categorise agreements into broad categories of risk at this stage, depending on the extent of the provisions that are included.

AUTHORS

Rebecca Cousin is a Partner and Cindy Knott Data Protection PSL at Slaughter and May.
Emails:
rebecca.cousin@slaughterandmay.com
cindy.knott@slaughterandmay.com

REFERENCE

1. curia.europa.eu/juris/liste.jsf?num=C-40/17

ICO seeks powers to seize assets

The ICO says it should be granted the power to seize assets and cash, and undertake financial investigations, including search and seizure warrants. The regulator argues that these powers are essential as personal data has a monetary value and is increasingly being recognised and treated as a commodity which is stolen and traded for financial gain. The powers could be granted to the ICO under the Proceeds of Crime Act 2002 (POCA), and the ICO has now put its proposals to a public consultation.

"The General Data Protection Regulation (GPDR) has introduced increased financial penalties for civil breaches of the Data Protection Act 2018 (DP Act 18). Criminal offences under the DP Act 18 are now recordable. However, the only sanction available to the courts following a criminal conviction is a fine, which in some cases will be much less than the financial gains made by the offender. This will inevitably lead to a greater disparity between the deterrent and punitive effects of sanctions imposed in relation to civil breaches and criminal offences," the ICO says.

POCA investigation and other associated powers would enable the ICO to assist the court in the identification of assets and to determine the value of a criminal's proceeds from crime. The ICO has previously worked in partnership with other agencies which conducted financial investigations on its behalf and assisted the courts with these cases. To date the ICO has prosecuted and convicted several individuals who were later stripped of assets by the courts using POCA confiscation powers. However, these partner agencies are no longer able to provide assistance, it says.

The powers the ICO is seeking are:
1. To apply to the court for Restraint Orders (under Part 2 of POCA);
2. To apply to the court for Confiscation Orders (under Part 2 of POCA);
3. Cash seizure, detention and forfeiture from premises (under Part 5, Chapter 3 of POCA);
4. Asset seizure and forfeiture from premises (under Part 5, Chapter 3A of POCA);
5. To undertake investigations (including search and seizure warrants) to support the proceedings sought above (under Part 8 of POCA); and
6. Access to information relevant to the investigation of money laundering offences.

• *This consultation closes on 6 December 2019. See ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-call-for-views-on-the-application-for-powers-under-the-poca/*

ICO issues opinion on live facial recognition by law enforcement

The first Opinion under DP Act 2018 was issued by the UK's Information Commissioner on 31 October 2019. **Aaminah Khan**, Barrister, analyses the issues at stake.

The Opinion sets out the ICO's position and makes recommendations relating to the use of Live Facial Recognition by police forces, following an ICO investigation into how the police use this technology in public spaces. A report of the ICO investigation findings, together with the Opinion, were both published on 31 October 2019. Considering that this is the first Opinion issued by the Commissioner under section 116 and Schedule 13 of the Data Protection Act 2018, since the commencement of the Act, it shows how high a priority this topic is for the ICO.

Live facial recognition technology processes, in real time, biometric data, allowing police to identify individuals as they pass facial recognition cameras, although non-live methods of identification, i.e. from older or still images are also utilised by the police. As it involves the processing of biometric data, live facial recognition is brought within the scope of the GDPR and the DP Act 2018, with police forces having to comply with Part 3 of the DP Act 2018 (law enforcement processing). The use of live facial recognition by law enforcement constitutes sensitive processing of biometric data under section 35 of the Act and as such is subject to greater safeguards under the Act. For example, the police have to demonstrate that the processing is strictly necessary, which is a higher bar than merely necessary, and further that a Schedule 8 DP Act 2018 condition is met. The use of this technology by police forces in recent times has been on the increase, having been used at events where large crowds of people are expected such as football stadiums and the Notting Hill Carnival.

Whilst this Opinion, the investigation and its recommendations focus on law enforcement, many of the privacy issues that this developing technology raises will come into play when the use of this technology is being considered by the private sector. It is clear that there is a growing interest from private sector organisations in facial recognition type technology, from shopping centres wanting to identify known shoplifters or individuals with retail exclusion orders to bars and nightclubs wanting to identify persons of interest, and it is easy to see why the use of facial recognition may be attractive to some businesses. It is also clear that this technology is a regulatory priority for the ICO, who have indicated that they are also investigating its use outside of the policing sphere.

ICO INVESTIGATION

The ICO report and Opinion follow a 17-month investigation into the use of live facial recognition by primarily South Wales Police and the Metropolitan Police Service (the Met). Aside from the ICO investigation, for several months Facial Recognition Technology (FRT) has also featured regularly in the media, from Kings Cross Estate using FRT for almost two years without the public being aware, to debate around the increasing use of FRT in shops and supermarkets.

During the course of the ICO's investigation, the use of FRT by South Wales Police led to the case of *R (Bridges) v Chief Constable of South Wales Police and Others*[1]. South Wales Police trialled live facial recognition technology in public spaces, in order to identify individuals who may be connected to criminal activity or at risk in some way, by scanning profiles and comparing against offender databases. Similar trials have been undertaken by other police forces, including the Met.

The technology processes the biometric data of potentially thousands of individuals who pass before the cameras. Some individuals will be stopped and spoken to by officers as a result, sometimes without justification, as the accuracy and effectiveness of the technology has been questioned, particularly in relation to some ethnic groups. The action of South Wales Police was challenged by way of Judicial Review in the case of *Bridges* by a member of the public, concerned about the lawfulness of the way his data had been processed whilst out shopping in Cardiff City Centre. The claimant was supported in his legal action by the civil liberties group Liberty.

The ICO has raised concerns over the invasiveness of the technology for

USE OF FACIAL RECOGNITION PROGRAMMES FALLS UNDER DP LAW

In its Opinion, issued on 31 October, the ICO says that data protection law applies to the whole process of live facial recognition (LFR), from consideration about the necessity and proportionality for deployment, the compilation of watchlists, the processing of the biometric data through to the retention and deletion of that data.

"Controllers must identify a lawful basis for the use of LFR. This should be identified and appropriately applied in conjunction with other available legislative instruments such as codes of practice," the ICO says.

Based on the judgement in *R (Bridges) v The Chief Constable of South Wales* [2019] and the evidence gathered in the ICO investigation, it says that there is no basis for regulatory action.

While there is some evidence of processing good practice by both South Wales Police (SWP) and the Metropolitan Police Service (MPS), there are areas of data protection compliance where the MPS and SWP could improve practices, share lessons and reduce inconsistency.

As there is an increased risk of compliance failure and undermining public confidence, the ICO says forces and other law enforcement agencies are advised to consider the points made in the Commissioner's opinion.

some time; the Commissioner has blogged about her concerns relating to the unnecessary intrusion and potential detriment that could be caused from the use of the technology, and the ICO intervened in the *Bridges* case as an interested party, making submissions to the Court. The High Court in *Bridges* did not consider that the processing was unlawful, rejecting the claimant's arguments that the processing carried out by South Wales Police was not in accordance with the law or proportionate. However the claimant has publicly confirmed that they have commenced an appeal against the decision. South Wales Police have subsequently continued to use the technology, although the recent use at a football match between Swansea City and Cardiff City was met with opposition from some football supporters who turned up wearing masks and with banners in protest.

Support from the public

Whilst the use of this technology is controversial, interestingly facial recognition does have relatively strong support from the general public. The ICO's investigation report revealed that there was strong public support for the use of live facial recognition for law enforcement purposes, with 82% of those asked (of a group of over 2,200 sampled) being of the view that it was acceptable for the police to use the technology. The results were also strong where it was suggested that only one person was being located, with 60% of those asked agreeing that it would be acceptable to process the faces of a crowd even if it was to locate only one person of interest, and a similarly large number (58%) thought it would be acceptable to be stopped by the police if erroneously matched. It therefore appears that, based on these results, the general public are supportive of the use of the technology in policing, although the ICO investigation report acknowledges that there is other research which has shown that the picture is not consistent across different groups in society, with lower support amongst certain groups. It would be interesting to know how public opinion would compare if asked about use of the technology in the private sector.

ICO proposes a statutory code

It could be said that we are sleepwalking even further into a surveillance society, similar to the concerns raised by the ICO in relation to the increasing use of CCTV technology over a decade ago. With the lawfulness of South Wales Police's use of FRT being confirmed by the High Court, subject to any appeal, it is likely to continue to be rolled out and increase in prevalence. One of the main recommendations in the Opinion is the Commissioner's call for the strengthening of the legal framework in this area, in order for there to be greater clarity, foreseeability and consistency in relation to the use of the technology, by the introduction of a statutory Code of Practice. The ICO recommends that the development of this Code be led by the government, making reference to the Surveillance Camera Code as an example. A statutory code would no doubt be welcome by many, as it would provide a clear framework for data controllers on how to carry out this processing in a way that is justifiable and proportionate, especially as this is one of the areas of developing technology where the legal framework and guidance is struggling to keep pace with the speed of technological advancement taking place. Further guidance of the use of this FRT in the private sector would also be particularly helpful, given the lack of specific available guidance in this area.

Whist the court in *Bridges* found the use of FRT to be lawful in that specific context, it has to be borne in mind that there exists a strong public interest for the use of FRT to prevent and detect crime, whereas some uses in the private sector will not necessarily justify the level of intrusion, therefore the principles of necessity and proportionality are key. In the Opinion, the Commissioner takes the view that whilst the High Court in *Bridges* found that the live facial recognition undertaken by South Wales Police was lawful, this should not be seen as a blanket authorisation to use the technology in all circumstances. Data controllers who are considering using facial recognition will also need to consider the lawful basis for processing carefully and determine the lawful basis before commencing processing. If consent is being considered as a potential basis, any power imbalance will of course be relevant – the ICO takes the view that it would be highly unlikely that consent would be a valid basis in the context of law enforcement.

> The ICO recommends that the development of this Code be led by the government, making reference to the Surveillance Camera Code as an example.

Appropriate policy document and DPIA needed

Organisations considering the introduction of this technology are advised to develop an appropriate policy document, setting out the justifications for use of the technology, in order to be able to demonstrate that its use is necessary and proportionate. In the investigation report, the ICO indicates that further guidance on appropriate policy documents is in the process of being developed.

Organisations are further advised to carry out a thorough data protection impact assessment (DPIA), which should also be well documented, to assess the impact that the processing will have on individuals and how these will be specifically addressed. The ICO's investigation report sets out a number of areas where the police DPIAs, which were reviewed as part of the investigation, could be improved with more detailed consideration about matters such as strict necessity and the proportionality considerations. One suggested area of improvement was greater involvement of the DPO, particularly in the earlier stages of the process. The ICO recommends that in respect of law enforcement agencies, DPIAs are provided to them in advance of roll out in order for early engagement with the regulator to take place.

A further recommendation of the ICO is in relation to the development of the technology's algorithms to ensure that they do not contain any technical bias, by treating certain

groups less favourably and to the extent that any technical bias may be present, that steps are taken to mitigate this factor. The ICO notes that any failure to address any such bias may have implications not only under the DP Act 2018 but also potentially for public bodies the Equality Act 2010. Fair processing information, including signage, will also be important to get right in this area, ensuring that signage is clear and that individuals are sufficiently informed of the processing being undertaken and also that data subjects are aware of how they can exercise their rights under the DP Act 2018 in relation to the processing.

With FRT such a contentious issue, this will be an area the ICO is expected to keep a close eye upon, and it may only be a matter of time before formal enforcement action is taken by the ICO in this area. Certainly, given the warnings from the UK Commissioner on how concerned she is about this issue, any data controller planning FRT who does not take compliance with the DPA and GDPR seriously ought not to be surprised if they find themselves subject to an ICO investigation. The ICO won't be the first to enforce on FRT however, as the Swedish data protection authority in August issued a GDPR penalty on this matter.[2] The case concerns a school that was piloting the use of FRT to monitor student's attendance and save teacher time in taking student register. The failings in this case relate to processing data in a more invasive manner than necessary (Article 5), processing sensitive personal data without a legal basis, consent not being valid (Article 9) and not complying with the requirements of DPIA and prior consultation with the Swedish DPA (Articles 35 and 36).

AUTHOR

Aaminah Khan is a Barrister at St John's Buildings.
Email: clerk@stjohnsbuildings.co.uk

INFORMATION

See ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf
ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf

REFERENCES

1 [2019] EWHC 2341 (Admin)
2 www.datainspektionen.se/nyheter/facial-recognition-in-school-renders-swedens-first-gdpr-fine/

ICO reminds political parties to stay within DP law

The Information Commissioner has written to the political parties in relation to the use of data in political campaigning at the general election. Elizabeth Denham wrote:

"As I set out in my letter to the political parties before the elections to the European Parliament in May 2019, the ICO's investigation into the use of data analytics for political purposes found a number of concerns relating to the use of commercial behavioural advertising techniques and the lack of transparency of profiling during recent political campaigns. The investigation identified a number of areas where action was required to improve each of the political parties' compliance with data protection law. I outlined these concerns in warning letters to political parties in July 2018."

"Following on from the warning letters, we carried out data protection audits on a number of political parties as we promised to do in our investigation report. We have been able to use some of the initial findings from these audits to improve our understanding of the data aspects of emerging campaigning techniques and current practice in political parties. We have used this knowledge to help inform our recently published draft framework code of practice for the use of personal information in political campaigning. This draft framework provides guidance on the practical application of data protection and electronic marketing laws to political campaigning practices."

She reminds the parties of data protection requirements and informs them about a specific website set up for advising political campaigners.

• *Advice to political campaigners is at ico.org.uk/for-organisations/in-your-sector/political/political-campaigning/*

Also see ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/11/information-commissioner-reminds-political-parties-they-must-comply-with-the-law-ahead-of-general-election/

'Half of organisations still not GDPR compliant'

The survey by Egress found that just over half (52%) of UK businesses are not fully GDPR compliant. A lower percentage (39.5%) of mid-sized companies reported full GDPR compliance compared with 56% of large and 51% of small companies. Also, 37% of respondents had reported an incident to the ICO in the past 12 months, with 17% having done so more than once.

Over one-third of respondents (35%) said GDPR has become less of a priority for their organisation in the last 12 months. Implementing new processes around the handling of sensitive data has been the greatest area for compliance investment in the last 12 months, said 28% of those surveyed.

The survey, which gathered views of 250 organisations of all sizes, was conducted in July 2019 by independent research organisation OnePoll on behalf of Egress.

• *See pages.egress.com/GDPR-survey-2019-uslp.html (requires providing personal details to download the free report)*
See also www.realwire.com/releases/UK-businesses-are-still-not-fully-GDPR-compliant-according-to-Egress-survey

ICO continues to invest in international cooperation

Laura Linkomies reports from the 41st International Conference of Data Protection and Privacy Commissioners (ICDPPC) which was held in Albania 21-24 October.

The ICO continues to play a key part in the international arena despite Brexit and the uncertainty over its role with EU counterparts. Closing the proceedings of the 41st International Conference of Data Protection and Privacy Commissioners in Albania, the UK's Information Commissioner, Elizabeth Denham, said that the conference now gathers together 120 jurisdictions. Decisions taken about the future of the conference include year-round cooperation, changing its name to Global Privacy Assembly, and opening up to engage more with external stakeholders, in particular civil society, in a new reference panel to be formed in 2020.

Denham, current Chair of the conference was confirmed to continue for the next two years. The ICO played an important part this year in assisting their Albanian colleagues to organise the conference.

The conference adopted several resolutions:

- on the promotion of new and long-term practical instruments and continued legal efforts for effective cooperation in cross-border enforcement;
- on privacy as a fundamental human right and a pre-condition for exercising other fundamental rights;
- to support and facilitate regulatory co-operation between data protection authorities and consumer protection and competition authorities to achieve clear and consistently high standards of data protection in the digital economy;
- to address the role of human error in personal data breaches;
- on social media and violent extremist content online.

In addition, the conference recognised children's online privacy as a key area of focus, as well as the challenge of developing the competence and skills children need. Members will share information and experiences on children's rights in relation to learning analytics technologies in the school environment, and the relationship to parental rights such as access to a child's health-related data and with reference to the UN Convention on the Rights of the Child. The ICDPPC notes that children's privacy is also currently an area of focus for the UN Special Rapporteur on the Right to Privacy, the OECD and the Council of Europe, and looks forward to collaborating.

Denham said: "We need the right kinds of laws so that online experience for children is fair. The forthcoming UK code is all about this."

Convergence and connectivity

Commenting on the importance of global coherence in data protection and privacy, Denham wrote in a blog: "As UK Information Commissioner, part of my role is contributing to global collaboration, to ultimately better protect people here in the UK. That work includes chairing the International Conference of Data Protection and Privacy Commissioners (ICDPPC)."

"Our focus this year is on convergence and connectivity – in our laws, in our standards, and in how regulators like the ICO can work with our counterpart regulators across borders. That is the only way we can keep our citizens' data safe. We'll be thinking about some of the fundamental challenges data protection regulators around the world are facing. How do we support consumers in our own countries, after a multinational company based thousands of miles away gets hacked? How do we make sure our voices are heard when privacy is a small part of an emerging international issue like cryptocurrency?"

In a press conference, she reflected on the importance of fines to drive compliance: "Fines are not enough. We need to use other tools and remedies too. The most effective way to change conduct may be to stop processing orders and reveal how business models work."

She said that the investigations into British Airways and Marriott data breaches, and the intention to fine them, are ongoing.

"We have received submissions from the companies. The notices of intent were made public by the companies themselves due to market pressure. We will conclude the investigation by end of the year."

Brexit

PL&B understands that the UK will not be able to take part in the meetings of the European Data Protection Board unless the issue at hand particularly concerns the UK when it could attend only as an observer. The ICO has published some guidance materials on its website for how to deal with data transfers after Brexit. The guidance includes specific tips for large organisations and SMEs.

Organisations may need to consider appointing a European representative if they are based in the UK and do not have a branch, office or other establishment in any other EU or European Economic Area (EEA) state, but offer goods or services to individuals in the EEA, or monitor the behaviour of individuals in the EEA (*PL&B UK Report* March 2019 p.1).

INFORMATION

The ICDPPC Resolutions are at icdppc.org/document-archive/adopted-resolutions/
ICO guidance on Brexit is at ico.org.uk/for-organisations/data-protection-and-brexit/

The future for charity fundraising: Innovation and data protection

Data protection for charities and the status of GDPR compliance. **Merrill Dresner** reports.

Richard Sisson, Senior Policy Officer, ICO, provided an overview of GDPR compliance and its impact on organisations, and the ICO. He said that complaints have doubled, and now stand at 41,000 per year. Breach reports have reached 14,000, whereas the year before the GDPR there were 3,000. There are now 700 staff, 60% more than in 2016, and an increased focus on particular areas of work, such as Codes of Conduct, online harms, age appropriate design and, inevitably, Brexit.

When the scandals emerged around personal information and political influencing, and the disruption of democracy itself, the ICO investigations concluded: "To retain the trust and confidence of the electorate, all of the organisations involved in political campaigning must use personal information in ways that are transparent, understood by people and lawful." Research commissioned by Ofcom into online harms found that:

- 79% of UK adult internet users have concerns about aspects of going online
- 66% are concerned about content
- 58% are concerned about data/privacy
- 55% are concerned about interactions with other users
- 54% are concerned about hacking/security
- 45% of UK adult internet users indicated that they have experienced some form of online harm
- 21% of UK adult internet users have taken action to report harmful content.

As a response, the ICO's Information Rights Strategic Plan (IRSP) from 2017 to 2021 sets the following goals, to:

1. Increase public trust in how data is used and made available.
2. Raise the standard of information rights through clear, inspiring and targeted engagement and influence.
3. Highlight the UK's place in the global rights environment and develop the UK's influence in the regulatory community.
4. Stay relevant to public concerns, especially where technology is concerned.
5. Enforce existing laws, and
6. Be an effective and knowledgeable regulator for cyber-related privacy issues.

The ICO's regulatory priorities are cybersecurity, AI, Big Data and machine learning, web and cross-device tracking for marketing purposes, children's privacy, surveillance and facial recognition, use of biometric data, data broking, use of information in political campaigns and Freedom of Information Act compliance.

The ICO's Regulatory Action Plan, said Sisson, aims to integrate ICO functions to provide an all-round better service. The changes have involved combining the advice and complaints departments, as the two were often linked in relation to their public service anyway, and also expanding high priority investigations and intelligence. Streamlining domestic strategic matters and high-priority relationships will further improve the ICO services.

The key word for the future is "enforcement," without which compliance becomes irrelevant, he said. Good practice points for the future are transparency, accountability and privacy by design and default. It is important for the ICO to emphasise that consent is not the silver bullet that the GDPR publicity may have led people to believe. Another good rule of thumb is only to ask for and keep the data that you need, and only use it because you need it, not for other reasons.

Questions to Sisson about the types of complaints coming from the charitable sector received the reply that they were mostly about Subject Access Requests (SARs). The number of these complaints used to be higher so this is a positive trend. The highest number of complaints about SARs are about companies or charities not responding in time.

Sisson said that a new DMA code of practice is due to appear in the autumn. He recognised that staff training is a challenge for small charities but would create more trust.

Are larger charities sleepwalking into problems around their use of consent as a legal basis? The top 15 charities are all profiling without consent and the smaller ones simply follow their lead. This could be a publicity disaster about to be revealed by the media. If the case warranted action, the ICO would take action, Sisson replied.

On record-keeping, the ICO's advice is to have a visible retention schedule and stick to it. On using cookies, Sisson referred to the ICO's guidelines. Although there may be a storm brewing as we wait for the EU e-Privacy Regulations, in the UK, the Privacy and Electronic Communications Regulations (PECR) still governs the use of cookies and should be closely followed.

Trends in digital marketing and fundraising

John Mitchison, Director of Policy and Compliance, Direct Marketing Association, said that the DMA has now officially changed its name to the Data and Marketing Organisation (DMO). It has 1,000 members split between suppliers, brands and members. Another arm of the DMA is called *DMA Talent* which services the data marketing community.

Mitchison explained that data flows have become extremely complicated, with Real Time Bidding (RTB) affecting dataflows and data leakage. After 2020/21 we will have EU e-Privacy Regulations, but for now, none of the changes are new, as they have evolved. The GDPR has also evolved from a rule-based law to a principle-based one. For the DMA this means an unwritten change of ownership of data – from the ownership of data by the

company to the position we have reached now where clearly the consumer owns their own data. "We look at what consumers think, and the good news is that the majority of people are happy with the amount of data they share" Mitchison said.

It was only recently that digital marketing came into the spotlight, and specifically with discussions on the Right to Be Forgotten (RTBF) that people are starting to think that technical stuff about data is now too difficult for the average person to understand. RTBF has shown us just how widely our data is shared – and how complicated it is to retrieve once it is out.

The ICO gave us an ultimatum and we have had six months to make progress, Mitchinson said. What was our biggest concern? It was that processing of special category data would normally need explicit consent. Where is the ICO going to focus its concerns on marketing?

On cookies, we need more clarity because, despite guidance which the ICO produced (3 July 2019), most people will need to make significant changes, Mitchinson said. All cookies are controlled by PECR which may be replaced by the EU e-Privacy Regulations (depending on whether UK is still in the EU) in 2021/22 and accompany the GDPR.

According to the current proposals, B2B consent will be required, Member States could decide a time restriction for the use of soft opt-in, telemarketing would require consent and a special prefix for marketing, and use of cookies would also require consent unless they are analytics cookies, Mitchison explained.

My advice to charities is "Don't ignore it – put some mechanism in place!"

Practitioners' view

A panel session discussed GDPR compliance, consent and best practice for data processing and use going forward.

Rowenna Fielding, Data Protection Lead, Protecture, explained that her organisation, when collecting views from 200 organisations, has discovered that there is a universal awareness of data protection and people have mostly heard of PECR. The attitude to data protection is now better than it was; rather than just complaining, people are not looking at just the bare minimum, and recognise that good corporate behaviour is a better standard to aim at than mere compliance.

Not only are ethics better understood, but also the rights and freedoms of data subjects. Aligning privacy messaging with communications strategy is the best way forward, and companies are now following this path, she said.

Data protection by Design and Default still are not being considered early enough. Data protection is a lot like gardening – it has to be done little and often and very frequently to prevent the bindweed from suffocating the garden.

Best practice goes into a culture of upholding ethics – it's hard work, costly, reduces the speed of manoeuvre but it is a worthwhile investment! At least these conversations about values are being held now, Fielding concluded

Carla Whalen, Senior Associate, Charity and Social Business Team, Russell-Cooke said that they get asked about lawful basis the most, but this is now changing slightly. 18 months ago, people thought that GDPR requires only consent but of course organisations can also rely on legitimate interest. Consent looks messy and it is hard to manage.

Now, some charities have moved away from consent for all types of marketing. PECR gives you no flexibility. E-marketing and SMS require consent but telemarketing and postal marketing both need checking for explicit consent (Telephone Preference Service), she said.

Charities find these specific and granular requirements really difficult and do not successfully split up the consents – people generally only get the chance to answer one question only, and then, if someone withdraws their consent, the charity loses all possibility of contact – there is no middle ground.

Whalen offered these conclusions:

1. If you use consent, think about the validity of that consent.
2. If you use legitimate interest, do an assessment for different categories e.g. differentiating between postal marketing and other forms – it will have to be very specific.
3. If you say "we will send you marketing with your consent" then stick with it – don't change the basis of their consent and don't change your practice."

Katie Simmons, Director, Fundraising Strategy, British Red Cross said that the Red Cross is a 150-year-old well known large charity with income of more than £140 million a year from donors. "We are highly dependent on large scale regular giving, and engaging with mass audiences, and were in the spotlight in 2015/16 when we were investigated by the ICO."

The impact of recent GDPR changes has meant challenges and opportunities. We present data protection as being not just about compliance, but also about supporter experience. We ask how people want to communicate with us, how to be cost effective, how to be more highly targeted. Diversification has helped us to explore new areas, she said.

"Our challenges have been to balance supporter needs with income generation, and here there is a lack of sector-wide leadership from bigger charities. There are the usual issues of consent versus legitimate interest, and data retention, and how to prospect for new major donors. SARs are a source of concern in that they use up resources."

"My thoughts about the future, apart from Brexit and keeping up with future regulations, are that evaluation and ongoing compliance need to be kept up.

Amanda Griffiths, Head of Communications Planning, Royal Mail MarketReach, explained that it is a branch within the Royal Mail, and is about mail, however it is sent – it puts mail at the front of marketing. "Mail still does very important things – it is highly tangible and personal," said Griffiths. "We see GDPR making mail stronger, because the data now available is for people who want to be contacted." This puts the customer more in control, making them aware that what they receive is what they want. The GDPR has led to a new mail option – Partially Addressed – that targets by postcode (narrowing addresses down to about 15 households), so it is highly targeted without using personal data. Mail now offers a choice of three interconnected ways to reach audiences – Direct Mail, Partially Addressed, and Door Drop.

In response to the question of whether postcodes are regarded as personal information, Griffiths said, "On their own, postcodes do not represent personal information because they combine about 15 households on average. Only in the very few cases across the UK where a postcode has only one household would a postcode represent personal information – so these post codes are not used for Partially Addressed Mail.

Partially Addressed Mail analyses the combined geodemographic characteristics of the grouping of all households in a post code. As a result, it can be highly targeted, but that targeting does not use personal data. The mail when sent is addressed not to a named individual but to a shared salutation for example, Occupier, Holiday Lover, Smart Shopper and so on.

She showed a video from the Movember charity, highlighting the success of the campaign which raises money for prostate cancer. Their "Shave the Date" campaign harnessed the power of mail, which for them was physical, personal, targeted and integrated. From a very small beginning, Movember are now looking for a global roll-out.

Confidence comes from having paperwork to back up the training, and being able to ask the question – what is a reasonable expectation of privacy from our donors? What is reasonable and what could be creepy is a very individual judgement.

Mitchison answered that it makes a difference the type of industry you are in and what you are asking. Whalen suggested that a DPIA is a good idea in case a campaign is "creepy" and might trigger questions. Fielding said that she applies "a good rule of thumb which is that if you wouldn't be happy doing it right in front of them, don't do it!"

INFORMATION

The Westminster Policy Forum, Future for charity fundraising – innovation, data protection and the impact of new regulation, was held in London on 31 October.
See
www.westminsterforumprojects.co.uk/conferences/westminster-social-policy-forum

US and UK sign agreement on access to law enforcement data

The United States and the United Kingdom have entered into an agreement that will allow American and UK law enforcement agencies, with appropriate authorisation, to demand electronic data regarding serious crime, including terrorism, child sexual abuse, and cybercrime, directly from technology companies based in the other country.

In 2018, the US enacted the Clarifying Lawful Overseas Use of Data Act (CLOUD) Act, which authorises the United States to enter into bilateral executive agreements with partners that lift each party's legal barriers to the other party's access to electronic data for certain criminal investigations. The US-UK treaty is intended to significantly reduce the timescales of investigations of serious crimes while assuring the protection of citizens' privacy, says the US Department of Justice. The current legal assistance process can take up to two years.

All requests for access to data under the new agreement will be subject to independent judicial authorization or oversight, and respect data protection laws, the parties say.

- *See www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists*

Brexit uncertainty for DP continues

If after the general election the UK leaves the EU with a Withdrawal Agreement and enters a transition period, there is no immediate change for data controllers. During that time, data flows to EU countries would continue as normal, and the government would be likely to negotiate an adequacy agreement with the EU. However, in case of a no-deal, organisations would need to rely on other tools such as Standard Contractual Clauses (SCCs), or Binding Corporate rules.

The government has issued some very general guidance in its No-Deal Readiness report. It says that organisations should visit GOV.UK and use the ICO guidance for further information on alternative transfer mechanisms and how to use them, and on the other, less critical steps they may need to take.

PL&B has learned from government sources that the DCMS is currently evaluating third countries' data protection frameworks in order to be able to issue its own adequacy decisions. It is not entirely clear whether these decisions would follow the EU's current adequacy decisions, or include countries that are not yet classified as EU adequate. By the end of October all the EU adequate jurisdictions had agreed to a mutual adequacy arrangement with the UK except Andorra.

- *See assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/837632/No_deal_readiness_paper.PDF*

Parliament's Committee on Human Rights: Consent model is broken

Parliament's Joint Committee on Human Rights says that the consent model is broken, and for the majority of individuals the information providing the details of what we are consenting to is too complicated to understand.

In its paper, The Right to Privacy (Article 8) and the Digital Revolution, published on 3 November 2019, the committee says that even when consent is given, all too often the limit of that consent is not respected. "We believe companies must make it much easier for us to understand how our data is used and shared. They must make it easier for us to 'opt out' of some or all of our data being used."

"It is unreasonable to place the onus for knowing about the risks or harms associated with using web-based services on the consumer. Internet users should be able to trust that the infrastructure is secure and will protect them appropriately. Consent should no longer be used as a blanket basis for processing."

The committee recommends that the government ensures that robust regulatory standards are in place, and rigorously enforced, so Internet users can be confident that any data that companies hold about them is being used in a reasonable manner.

"Given that there is a lack of understanding among companies around the use and relevance of the legitimate interests basis, we consider that there should be clearer guidance to companies either issued from the ICO or the government around when and how the legitimate interests basis can be used. We also consider that there should be a rigorous process to test whether companies are using legitimate interests appropriately."

The government should look at creating a single online registry that would allow people to see, in real time, all the companies that hold personal data on them, and what data they hold, the committee suggests.

The committee received 31 written submissions. It also took oral evidence from a range of witnesses including the Information Commissioner's Office, industry representatives, data brokers and Google, as well as specialist lawyers, academics, and journalists.

- *See publications.parliament.uk/pa/jt201920/jtselect/jtrights/122/122.pdf*

Un-checking a box is not valid consent

The 1 October ruling from the Court of Justice of the European Union (CJEU) deals with ways that consent can be obtained on the Internet, and tracking cookies for analytics or marketing purposes on websites. "In the opinion of the CJEU, consent is not valid if the storage of information via a cookie is consented to by means of a pre-ticked box that users have to untick if they do not want to give their consent (so-called opt-out)," Oppenhoff & Partner reports.

The *Planet49* case concerns a German Federal Court referring several questions to the CJEU regarding the validity of consent to cookies placed by a website which was operating an online lottery. No GDPR-style consent was obtained. It was assumed that consent was given by further use of the website.

"In his final opinion, the Advocate-General of the CJEU took the view that the setting of third-party cookies (in particular, for advertising and analytics purposes) that are technically not required for the use of the website requires the active consent of the user. According to the Advocate-General, this applies both according to the former legal situation under the Federal Data Protection Act (BDSG) and/or Germany's Telemedia Act as well as under the requirements of the GDPR," Jürgen Hartung, Partner, Oppenhoff & Partner, Cologne, writes.

According to this ruling, consent must be actively given and specific - it must relate specifically to the processing of the data in question and cannot be inferred from an indication of the data subject's wishes for other purposes.

"Several data protection supervisory authorities also hold that pursuant to the GDPR the use of cookies for certain purposes is only permissible on the basis of the active consent of the users. The German Data Protection Conference (DSK) in its Guidance for Telemedia Providers has pointed out that, in principle, the use of technically not required cookies is only permissible with the valid consent of the user. This assessment is also shared by the French and Dutch Data Protection Authorities as well as by the ICO in the UK. For the legal assessment of the supervisory authorities, the technical procedures used or the type of cookies used are not the decisive criterion, but rather the purpose of the processing. The authorities have divided the various potential purposes for the use of cookies into certain categories: functionality, range measurement (analytics), and (marketing) tracking. In the opinion of the Data Protection Authorities, consent to the use of cookies is always required, unless they are technically required for the provision of the website functions," Hartung says.

The main consequences are:

- The use of cookies for analytics and marketing purposes with the now common "cookie banners" no longer complies with the requirements of the GDPR and the EU e-Privacy Directive.
- Before using these cookies, the user must give his or her consent in accordance with the requirements of the GDPR.
- Consent management solutions (or "cookie walls") might be required in the future, that effectively obtain and adequately document such consent.
- The data protection notice previously used must be updated regarding the use of cookies.

- *See 80884.seu1.cleverreach.com/m/7387665/0-ec240ab543c3edc201ea9a5b8ee33047*

Royal Free and Google DeepMind: A question of implied consent

Two years after the Royal Free Hospital's undertaking to the ICO on Google DeepMind Health's processing of its personal data, what can we learn from its audit and independent review? **Robert Waixel** reports.

In July 2017, the Royal Free Hospital (RF) was required by the ICO to sign an Undertaking[1] regarding the processing of its patient data by Google DeepMind Health (DM). Among the remedial steps required were an audit of the Royal Free and DeepMind's use of its data, and the establishment of an Independent Review Panel which would publish reports annually.

Peter Church, Counsel at Linklaters spoke, at the *Privacy Laws & Business* 32nd Annual International Conference, in Cambridge, about the audit and *Dr Julian Huppert, former MP and Director, Intellectual Forum, Jesus College, Cambridge University*, who was a member of the Independent Review Panel, talked about the Panel.

Why did Royal Free need to data mine its patient data?

Church began by reminding his audience why the Royal Free Hospital (RF) had brought in DeepMind Health (DM) to analyse its patient data to try and help sufferers of Acute Kidney Injury (AKI).

AKI is a serious health condition, with the elderly most at risk. It is associated with around 100,000 deaths a year in secondary care, and some 25% to 33% of these are potentially preventable. Such prevention could of course have massive benefits to the patients, their family, and provide yearly savings of £130m to £186m for the NHS, as AKI is part of about one in five emergency admissions to hospitals.

The Royal Free Hospital already had software called Streams which automatically gave an alert when a patient's blood test indicated AKI and provided contextual information for clinicians treating the patient. This was traditional decision tree/algorithmic based software, so neither Artificial intelligence (AI) nor big data/data mining were involved in this application.

RF wanted to go a step further in its app development and use DM on its patient data (of both patients with AKI and those without) to try and determine possible unknown causal influences of AKI in order to better understand who might be most at risk.

In a study jointly conducted by the ICO and the National Institute for Health Research (NIHR) Manchester in 2019[2], on the public attitude to using AI in healthcare, it was seen that the general public was relatively relaxed about organisations using deep learning AI techniques for stroke or kidney transplant scenarios, provided it was as or more accurate than by humans, even if there was a low transparency level of how the outcomes were achieved.

So where was the problem?

DeepMind were clearly a data processor and could only use patient information supplied by Royal Free under the latter's instructions. Assessing the contractual relationship using the ICO's advice on determining whether they were a data controller or a processor, they clearly fell under the latter on all criteria.

The question was raised whether the parties were joint data controllers on the basis of the *Wirtschaftsakademie* CJEU[3] case? Church was clear in his view that this ruling was inapplicable to these facts as DeepMind met all the regulator's criteria to be a data processor.

Under the common law duty of confidence, there was implied consent that patient data held by RF (and disclosed to DM) would be used for their direct care. In the design and development of the DM system for AKI for RF, synthetic data rather than real patient data was used. This was also used in the early part of testing. But, in the later stages of testing, a subset of real patient data was used, as the system needed to be tested with larger volumes, and only real data would provide the variety and richness that the system would need to deal with. This interim stage was problematic as there was no "direct care" relationship, thus no "implied consent". Once the DeepMind system was actually deployed, then both "direct care" and "implied consent" would kick in once again.

Would data minimisation be an answer?

Was there scope for data minimisation – that is restricting the data that was to be fed into the DeepMind datasets? This was discussed with the physicians in the hospital but it was felt that the whole purpose was to find unexpected relationships in the data which might be causal for or diagnostic of AKI. Previous research had already found unexpected data links to AKI so nothing could be easily ruled out of the data set mix at least at present.

Independent audit as a regulatory remedy

Specifying an independent audit as part of a regulatory remedy is a relatively unusual step in the UK, and this case was the first time the ICO had mandated a private audit. Church was part of the legal team conducting the audit. The advantages were the independence of the process and the specialist expertise that could be brought to bear on the issues. The audit was purely of the RF, and was only commenced shortly before the Undertakings were finalised. Therefore, the original arrangements with DM were already in place. The audit of the Streams system was carried out in the 12 months leading up to the GDPR so the auditors could only look back at pre-GDPR arrangements. Feedback to date on the audit report[4] has not cast any doubt on its factual or legal findings, nor the conclusions that the RF's use of Streams was legal.

Big Tech meets Health Tech

How far are the "Big Tech" companies trusted with personal data in general and health data in particular? This is not a new issue, as the issues causing the NHS to abandon[5] its *care.data* scheme in 2016 showed. One approach might be to aim for more radical transparency, new governance and accountability. Examples of this are the Monzo Bank's[6] financial app, embodying transparency by design, or the Yoti[7] (Your Digital Identity) external guardianship app which is already being used to check IDs in nightclubs, supermarkets and for the government of Jersey.

DeepMind Health Panel of Independent Reviewers

Huppert was a member of the DeepMind Health Panel of Independent Reviewers[8]. This was another oversight mechanism established by RF's Undertaking with the ICO. It was specifically tasked to look at the DM-Health and Royal Free Streams activities and was required to issue public annual reports.

The well-respected panel of reviewers had a broad range of skills and experience, with both real and perceived independence of Google, NHS and the regulators. They had complete access to all parts of DeepMind Health with no confidentiality obligations or Non-Disclosure Agreements (NDAs). The Panel was free to determine its own investigatory lines of inquiry with no control over its operations or report contents by Google or DeepMind Health. DeepMind Health were given a draft copy of the Report seven days ahead of publication to flag any factual errors but otherwise had no say.

Independent Review Panel's Annual Reports

The Panel has published two Annual Reports, in June 2017[9] and June 2018[10], but in November 2018 it was announced[11] that the panel would be abolished, due to the merger of Google DeepMind's Streams team with Google's translational health research team.

Translational research is the process of applying knowledge from basic biology and clinical trials to techniques and tools that address critical medical needs. Unlike applied sciences, translational research is specifically designed to improve health outcomes.

The First Annual Report, in June 2017, covered DM's Patient and Public engagement (now considered a gold standard for such activities) and the process of Design for Usability - to reduce and if possible, eliminate user errors. An external Security Audit was commissioned, but only the section on Alphabet's security was published.

A summary table of the number of vulnerabilities in Streams Apple IOS (Internet Operating Systems) apps, Web APIs (Application Programme Interface), Datacentre server build and Datacentre development by risk level, showed that there were only 11 vulnerabilities detected, all low or medium risks and no high or critical risk ones. The usual caveat was made about the possible presence of undetected or unknown vulnerabilities.

The Second Annual Report, in June 2018, provided 12 Principles for DeepMind Health and other Healthcare Technology companies[12] to follow, together with DeepMind Health's own self-assessment[13] against these criteria.

Did this approach work?

In Huppert's view the answer was "Yes". The Panel definitely made a difference to the DeepMind Health organisation particularly in the area of transparency. There were steps towards boosting the organisation's trustworthiness, but in Huppert's view, not enough happened to shift the wider narrative or to have a route to improve trust in the two-and-a-half years before the operation was taken over by Google Health. The journalistic narrative was unfortunately always set to highlight problems with the whole concept of AI and health data.

WHAT DID THE ICO SAY?

The ICO ruled in 2017 that testing the app with real patient data went beyond Royal Free Hospital's authority, especially in terms of the scope of the data transfer. It said at the time: "A patient presenting at accident and emergency within the last five years to receive treatment, or a person who engages with radiology services and who has had little or no prior engagement with the Trust, would not reasonably expect their data to be accessible to a third party for the testing of a new mobile application, however positive the aims of that application may be."

AUTHOR

Robert Waixel is an Associate Lecturer at Anglia Ruskin University and as RW Systems an independent consultant, tutor and speaker. He has been part of the Privacy Laws & Business team of conference reporters continuously since 1995.

REFERENCES

1 ico.org.uk/action-weve-taken/enforcement/metropolitan-police-service-june-2019/ ico.org.uk/media/action-weve-taken/undertakings/2014353/undertaking-cover-letter-revised-04072017-to-first-person.pdf
2 PSTRC, Citizen's Jury on AI, www.patientsafety.manchester.ac.uk/research/themes/safety-informatics/citizens-juries/
3 *Wirtschaftsakademie, Schleswig Holstein* (CJEU Grand Chamber case no C-210/16) 5 June 2018 curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=EN
4 Linklaters, Audit of the acute kidney injury detection system known as Streams at Royal Free Hospital, s3-eu-west-1.amazonaws.com/files.royalfree.nhs.uk/Reporting/Streams_Report.pdf 17 May 2018
5 NHS Executive, NHS England to close care.data programme following Caldicott Review, www.nationalhealthexecutive.com/Health-Care-News/nhs-england-to-close-caredata-programme-following-caldicott-review 7 July 2016
6 monzo.com/about/
7 www.yoti.com/
8 deepmind.com/applied/deepmind-health/transparency-independent-reviewers/independent-reviewers/
9 deepmind.com/documents/84/DeepMind%20Health%20Independent%20Review%20Annual%20Report.pdf
10 deepmind.com/documents/214/DeepMind%20Health%20%E2%80%93%C2%A0%20Independent%20Reviewers%20Report%202018.pdf
11 deepmind.com/blog/scaling-streams-google/
12 DeepMind Healthcare, Independent Reviewers Report 2018, June 2018, Page 7
13 DeepMind Healthcare, Independent Reviewers Report 2018, June 2018, Page 8

The data breach forest: Identifying all the trees

Robert Waixel reports on a panel discussion on issues and remedies following a data breach.

A session at the *Privacy Laws & Business* 32nd Annual Conference, at St. John's College, Cambridge, July 2019 focused on practical insights into data breach workstreams – other than notification – and how they all interacted with each other. The panel consisted of *Carl Blake, Legal Director at BUPA Global, Ioan Peters, Associate MD for Incident Response, Kroll*, and *Richard Jeens, Partner at Slaughter and May*.

Jeens advised that injunctions were a useful part of a data breach toolkit. They could be used at a very early stage of a data breach incident, if appropriate. A Court Order or injunction can be very powerful and deployed very rapidly (24/7 in the UK). An Order can be obtained, at the Court's discretion, for example, to stop people taking or distributing your data, or to stop someone who is receiving your data (such as a newspaper, other media or a competitor) using or exploiting it.

Alternatively, Court Orders can be used to require people to positively do things, such as an ISP to shut down a data source, or third parties to hand over details of bank accounts.

They can be obtained against "persons unknown" and can be obtained on a confidential basis, with all parties anonymised. A cause of action needs to be provided to the Court with evidence, and the process has to be claimed "in good faith". The claimant needs to think about how such an Order could be served on the defendant(s), and which other third parties should be given notice of it (e.g. banks).

Obviously, in due course, whatever injunction is obtained immediately, it will have to be eventually fully justified as an ongoing legal action at a later date to the Court, with notice to the defendant(s) who would then be able to be represented in their own right.

Show me some evidence?

Evidence will be needed both to obtain the injunction and to clarify what the order should encompass. Peters emphasised that "technical evidence is really helpful in substantiating the story to the Court, so that they know it is based on fact as far as is then known." He said "It needs to be gathered carefully – ideally by a third party – to avoid the perception of a conflict of interest." Other factors needed are to maintain a chain of evidence, and continuity of evidence, preserving the integrity of the evidence in court. Evidence and actions to gather it need to be justifiable as reasonable, proportionate, acting with good intent and the claimant needs to be able to demonstrate that in Court if necessary.

The types of evidence gathered vary. If the suspect was an insider, as much evidence as possible that can be lawfully obtained should be gathered and examined from both inside and outside the network. In any case, independent external digital forensic advice is absolutely essential as soon as possible, before well-meaning but forensically inexperienced local IT "experts" destroy vital evidence in their efforts to seek possible perpetrators out or to restore damaged systems as soon as possible.

Persons unknown injunction

Peters continued that a "Persons unknown" injunction can be really useful in arranging take-down notices, to avoid publication of trade secrets or contractually confidential information. ISPs worldwide will generally regard a take-down notice much more seriously if it is accompanied by an injunction, showing that the Courts have recognised a potential crime has occurred. It can also help with getting others to assist with an investigation.

Blake explained that with a rogue employee scenario at BUPA, and sensitive heath data at risk, it was imperative to take whatever steps were possible to stop such data being spread any further. It was also a way of gaining access to further evidence of what had happened at an early stage in the enquiry, from people holding other devices and from other organisations. However, BUPA needed to take the hard and conscious decision, rapidly, whether it was right to sue its own employee, as this was not a step to be entered into lightly.

The IT investigation

Jeens went on to explain that any such data breach investigation was likely to cover both internal and external aspects, and how important it was for a third-party IT forensic specialist, appointed under general terms, to be available 24/7 including weekends, and to be available on site, ideally, in under six hours from callout. Under GDPR, notification to the regulator must occur within 72 hours of 'being aware' of a possible data breach - further details can follow later.

Peters took up the theme. It is really important that organisations distinguish between the relative strengths of each team. An internal team knows the internal systems and can identify detrimental impact. But the bottom has fallen out of their world, and so they are likely to be emotionally conflicted and involved. There are also likely to be real conflicts between an internal team's natural instincts to 'put things right' and get on with or restore 'business as usual' and the need to identify and preserve evidence. An internal team will often destroy or contaminate such evidence, inadvertently.

External teams may not just consist of IT forensic experts, but also legal and PR resources, because all these skills will be needed in abundance to manage an incident. An IT responder, in addition to deep technical skills, needs to be able to think from the perspective of the adversary, and to be able to prioritise the information to be gathered at the scene, to process it, and preserve evidence that might be used in legal proceedings (including immediately for injunctions). Once this has been done, there needs to be an agreed

strategy to limit the damage, to inform stakeholders and regulators, and to start retrieving the situation.

The investigation report

Peters then turned to the Investigation Report. This document needs to be written to inform the Court in any future proceedings. It also needs to take into account privilege, and possible future regulatory action. It needs to be kept factual so that any experts from other parties can review the evidence and hopefully come to the same conclusions. But the facts have to be presented as part of a story that can be understood from the viewpoint of lawyers and non-technical people. Fact needs to be clearly separated from substantiated opinion, with no unsubstantiated opinion i.e. guesswork. Its structure needs to answer the questions of various stakeholders, including a range of regulators, including those from privacy and financial areas where appropriate. Peters then recommended that it should also include helpful factual advice on recovery, and how to prevent and fix any systemic errors that might have been part of the causation chain for the data breach.

Jeens agreed that the Report itself was unlikely to be considered a privileged document, certainly not if prepared in an advisory rather than in a purely litigation scenario. The internal team may well be tempted to take leaps from the proven facts, that an independent forensic investigator cannot do, and there needs to be no divergence in views, possibly discoverable within internal email exchanges, that could be exploited by other, opposing, parties. If there is to be speculation beyond the supported evidential base, then perhaps this is best placed in a clearly labelled separate document.

The external team needs to coordinate and work efficiently with the internal IT team, which can be difficult if they are seen to be "hindering rapid recovery" or "seeking to cast blame". Blake agreed, saying the scope of each party needed to be clearly set out and clearly there are likely to be tensions, particularly with the internal IT team having suffered what they will take to be a personal and professional intrusion. Internal IT may also be issuing reports filled with jargon (e.g. "Threat Actor") which are unhelpful for senior Management, legal or eventually, courts to comprehend. Cost is an issue for most clients, as external IT forensic teams are expensive, and the Board's willingness to pay, or not, is a good guide for how seriously they take the issue of a security and data breach. Cost and scope are of course related issues, and the wider the scope of external consultants, the higher the cost is likely to be. But the scope of the investigation may change over time, as more is learned.

Employment issues v data breaches

Although many data breaches originate from actions of internal sources (usually employees) many are accidental rather than malicious. Jeens acknowledged this in that it was always a difficult balancing act particularly for internal IT staff, as their world had just fallen apart (often literally), and there was a tendency, especially from Management, of looking for "someone to blame". There is also pressure to react quickly to put things back together again. So, the process of giving everyone 'fair and proper treatment' needs to be balanced against the potential risks of further harm to the organisation of not acting quickly enough. Often it is difficult to initially distinguish between a rogue employee acting in revenge, as against someone breaking the rules in order to 'get the job done' despite the restraints imposed by a clunky IT system. Both situations involve breaking the rules, but different levels of penalty might well be appropriate. This is why HR professionals (internal or external) need to be involved from the outset.

As always, the situation is more complex if it spans time-zones, jurisdictions or responsibilities. This is where a pre-prepared up to date crisis management plan or incident response plan really pays off, so that all appropriate departments are notified, and pre-identified external agencies are called in, regardless of which part of the organisation originally discovers or suspects the data breach.

It may be that different sets of regulators would wish to become involved, and if the employee has been summarily fired, that could add to their difficulties.

Once one or more internal suspects has been identified, they need to be found – which could be difficult if they are on leave, or in a job requiring mobility. Once you have found their work-related devices, can you as an organisation still get access to them? A suspected employee is not necessarily the guilty party – the initial evidence may be wrong or misleading, so the employee's rights must be respected whilst proceeding with any investigation. Decisions need to be clearly documented, together with the reasoning behind them and who was involved, as they may well need to be re-run in public in a courtroom in the cold light of day many months later.

Can IT forensics help?

Peters agreed that it was important for IT Forensics to preserve evidence as the story and the organisation's understanding shifts throughout the investigation. If employees have a right to use their own devices for work purposes, has the organisation a right to access that data and if necessary, to obtain the password/key? This may not be possible in all jurisdictions. Whatever the employee's story, can it be tested and proven as plausible or not?

AUTHOR

Robert Waixel is an Associate Lecturer at Anglia Ruskin University and as RW Systems an independent consultant, tutor and speaker. He has been part of the Privacy Laws & Business team of conference reporters continuously since 1995.

Significant changes to media, communications and data claims

A new regime for media, communications and data claims is now in force in the English courts, with the introduction of revised procedural rules and detailed practice directions. By **Simon Airey** and **Jack Thorne** of Paul Hastings LLP.

While defamation and privacy cases are certainly on the rise in recent years, data protection has become a particularly fertile ground for disputes, especially since the introduction of the GDPR. This trend is likely to continue. Large-scale data breaches are becoming increasingly common and give rise to potential multi-claimant actions brought by individuals whose data has been compromised as a result. These actions are being led by specialist law firms who have recognised the substantial growth of claims in this area and market themselves as data breach compensation experts, acting for claimants on a no-win- no-fee basis.

The procedural changes demonstrate not only a shift in the nature of the work being undertaken by the Courts, but also an understanding by the Courts that claims involving areas such as data protection encompass complex matters of law, for which specialist judges and a streamlined litigation process are required.

The changes were introduced on 1 October 2019 and include:

- a new Civil Procedure Rule (CPR) Part 53[1], which designates the Media and Communications List (the MC List) as a specialist list of the High Court where High Court claims for defamation, misuse of private information, breaches of data protection law, and harassment must be issued;
- two new practice directions (53A and 53B), which include rules concerning the transfer of proceedings to or from the MC List and the contents of statements of case; and
- a new pre-action protocol, which includes requirements regarding the contents of letters of claim in defamation, slander and malicious falsehood, privacy and confidence, data protection and harassment cases, and contains provisions dealing with responses to letters of claim and settlement/alternative dispute resolution.

> The new regime ushers in welcome changes at a time when claims relating to issues such as defamation, privacy and data protection are increasingly prevalent.

Designation as a specialist list

The MC List is not new. It was originally established in 2017 as a new list within the Queen's Bench Division (QBD). It was placed under the charge of Mr. Justice Warby, who was given primary responsibility for cases involving one or more of the main media torts (defamation, misuse of private information and breach of data protection law) and related or similar claims, including malicious falsehood and harassment.

Importantly, the MC List was not established as a designated specialist list and no specific rule required claims concerning defamation, privacy and data protection to be issued there. This was noted by Chief Master Marsh in *Mezvinsky & Ors v Associated Newspapers Limited* [2018] EWHC 1261 (Ch)[2], a case involving claims for breach of confidence/privacy and misuse of private information brought by the grandchildren of former US President Bill Clinton. The proceedings were issued in the Business List of the Chancery Division (ChD). However, given their nature, the Defendant made an application to transfer them to the MC List. The application was dismissed by the Chief Master, who observed that "unless the CPR expressly provides that an area of business is a specialist list…the notion has no application". He held that the MC List is not a specialist list: "It was not created by a provision in the CPR, or in statute" and that "The creation of the M&CL has no direct extra-divisional effect".

From 1 October 2019, this changed. Under the new CPR 53.2(1), the MC List will be made a designated specialist list of the High Court. However, more significantly, under new CPR 53.1(3), a High Court claim must be issued in the MC List if it is or includes a claim for defamation, misuse of private information, breach of data protection law or harassment by publication. In addition, a claim may be issued in the MC List if it arises from the publication, or threatened publication, of information via the media, online or in speech or other activities of the media.

Under new CPR 53.2(2) – (4):

- the judge in charge of the MC List will be a judge of the QBD. The position is currently held by Mr. Justice Warby;
- a formal category of judges in the MC List will be created (MC List Judges). The MC List Judges must be authorised by the President of the QBD, in consultation with the Chancellor of the High Court; and
- all proceedings in the MC List will be heard by MC List Judges or a Master of the QBD, although another judge of the QBD or the Chancery Division may hear an urgent application if an MC List Judge is unavailable.

The new practice directions

Two new practice directions will be introduced to supplement CPR 53.

PD 53A makes provision for the transfer of proceedings to and from the MC List. Any application for a transfer to or from the MC List must be made promptly and normally no later than the first case management conference. Where an application is made to transfer a claim to the MC List, an order for transfer will not be given until the judge in the MC List is satisfied that notice of the application has been given to the court in which the claim was proceeding and any applicable consent has been given. When considering whether to transfer a claim to or from the MC List, the judge in the MC List will consider whether the claim, or any part of it, falls outside of the scope of that list or falls within the scope of that list but would more conveniently be dealt with in another court or list.

PD 53B revises the current PD 53 to extend its application beyond defamation claims. So far as defamation claims are concerned, the new PD 53B reflects the current provisions of PD 53 concerning statements of case in such claims, the court's powers in relation to an offer of amends, applications for determination of meaning, summary disposal and statements in open court. However, the new PD 53B is extended to include broad provisions covering general matters regarding statements of case, as well as specific requirements for the contents of statements of case in claims for misuse of private or confidential information, breaches of data protection law and harassment.

It should also be noted that PD 53B states that CPR 65.28, which requires claims of harassment to be issued under the Part 8 procedure, shall not apply to claims for harassment arising from publication or threatened publication via the media, online or in speech. Accordingly, such claims will need to be issued under the Part 7 procedure.

The new pre-action protocol

A new pre-action protocol will be introduced to replace the current pre-action protocol for defamation claims. The new protocol will apply to all claims in defamation, misuse of private information, data protection law or harassment by publication, and claims in breach of confidence and malicious falsehood, which arise from publication or threatened publication by the print or broadcast media, online, on social media or in speech.

The new protocol includes provisions concerning litigants in person and specific requirements for letters of claim in cases involving defamation, privacy and breach of confidence, breaches of data protection law and harassment where the course of conduct includes publication. It also includes new provisions concerning settlement, and, specifically, the use of Part 36 offers to settle, as well as revisions to previous provisions concerning alternative dispute resolution.

Comment

The new regime recognises an expanding landscape in media and communications disputes.

While there are already specific rules and a pre-action protocol for defamation claims, the changes that were brought in from 1 October 2019 are significant as they revise and expand these rules and protocol to apply to a broader range of media-related claims, including those concerning data protection and privacy and confidence.

While claims in these areas are not new, they have increased markedly in recent years. This is not surprising in an age where the use of online content, social media and blogs has increased the channels through which, for example, potentially defamatory material and actions constituting harassment might arise.

Increasing issues concerning the mistreatment of personal data have meant that disputes relating to breaches of data protection legislation, and associated claims concerning privacy and misuse of private information, are now more prevalent than ever. This is primarily due to the imposition of the GDPR and Data Protection Act 2018, but also reflects the increased publicity and general awareness of how personal data should be handled. The upward trend of disputes in this area is unlikely to ease off, particularly given the frequency of significant data breaches and the establishment of specialist law firms focused on bringing large-scale compensation actions on behalf of claimants whose data has been compromised (p.1).

The requirement that data protection claims be issued in one list presided over by specialist judges means that cases in this complex, and still relatively uncertain, area of law will be determined by judges with appropriate expertise and experience in often self-contained issues. Further, the introduction of prescribed rules for dealing with such claims should ensure that they benefit from more consistent and efficient case management.

It is worth noting, in particular, that even though the MC List was originally established for the purpose of taking primary responsibility for media-related claims, claims based on areas such as data protection (and privacy) have continued to be issued in the Chancery Division, as well as QBD, with transfers to the MC List often refused. This has created uncertainty and arguably negated the purpose for which the MC List was originally created. The designation of the MC List as a specialist list and the requirement that claims concerning breaches of data protection law, misuse of private information, defamation and harassment be issued there, resolves this issue.

AUTHORS

Simon Airey is a Litigation and Regulatory Partner, and Jack Thorne is a Litigation Associate, in the London office of Paul Hastings LLP.
Emails: simonairey@paulhastings.com
jackthorne@paulhastings.com

REFERENCES

1 www.justice.gov.uk/courts/procedure-rules/civil/rules/part53
2 www.bailii.org/ew/cases/EWHC/Ch/2018/1261.html

Channel 4 creates a culture of privacy in the workplace

Stewart Dresner reports on the TV station's efforts to keep up with the GDPR's requirements.

Channel 4 is a public service television service entirely self-funded and reliant on advertising revenue to deliver its remit and licence obligations. Its statutory remit to innovate and present alternative views provides a different context to data protection compliance compared with the much larger publicly funded BBC. The main types of personal data processed by Channel 4 are for: All4, (the company's video-on-demand service); programme making; advertising; competitions; Human Resources, and marketing.

The starting point for Tamara Ballard, Senior Data Privacy Lawyer, together with the Channel 4 Privacy team, was to make data protection relevant for everyone in the business (staff, contributors, viewers and suppliers), plan a communications strategy, and find ways of ensuring that data protection is embedded in every new project.

Ballard generally runs small training sessions and for just a few people if the subject is specialist, for example, for adtech projects. The Channel 4 Privacy team won the support of the Channel 4 Exec who requires all staff, directors, heads of departments, and other managers to attend training sessions. Some of the Channel 4 Exec group speak at these sessions two or three times a year. In addition, she attends the Data Strategy Forum and the Exec-led Data Governance Forum. The Channel 4 Exec agreed an unusual incentive for staff to pay attention. Those who were the first to complete the online GDPR training in time (when first rolled out in May 2018) had the opportunity to win an additional day of holiday.

As in many other organisations, Ballard has appointed data champions who she trains every two months. They are responsible for raising awareness and promoting/providing training within their departments including working towards embedding data protection principles with their respective departments as well as documenting all data protection activities. As a result, if a department is audited, there is a record of what each department has been doing. She has centralised information resources in a Knowledge Management Privacy Compliance Hub.

Ballard explained: "We conducted our own audit of our data processors by asking each processor to complete a Data Protection Impact Assessment (DPIA), and updated all our data processing contracts to ensure they adhered to the processing clauses as required under the GDPR."

Engagement with the ICO

Channel 4 has engaged with the ICO by inviting them to Channel 4 prior to the implementation of the GDPR, and responding to ICO consultations, for example, the consultation on the journalism code and the Age Appropriate Design Code.

In addition, Ballard started an initiative the Public Service Broadcasters Roundtable, together with Field Fisher Waterhouse in 2016, to gather lawyers from the media industry to discuss, in a confidential environment, the challenges they faced with GDPR. She recommends using lawyers who really understand the broadcasting and media industry.

The campaign to encourage viewers to register for All 4 has led to a thorough review of its collection and use of personal data. Ballard had to balance the interests of the rights of the individuals and the needs of the company and its advertisers to conduct more targeted advertising. As a trusted and well-respected public service broadcaster, Ballard explained that Channel 4 ensures that All 4 user data is safe and secure and that Channel 4 have robust practices in place. It is evident that the more targeted the advertising, the greater opportunity to increase advertising fees which in turn creates funding for Channel 4 content. However, Ballard explained that Channel 4 does not collect sensitive personal data and that All 4 viewers have an understanding that Channel 4 is reliant on funding from advertising for how it creates and distributes its content.

The Channel 4 Privacy team ensured transparency requirements are met for All 4 registered users through privacy notices and award-winning marketing campaigns such as Alan Carr's Viewer Promise and the current Channel 4 video 'Your Data' which Ballard highlighted at the start of her presentation.

Data Protection Impact Assessments

The Channel 4 Privacy team started using DPIAs before they became a legal requirement. Ballard finds that they enable the business to think carefully about the collection and use of personal data before a project is launched. However, she acknowledges that it has been a challenge to create a template which is easy to use and understand.

Accountability

The need to create an accountability framework has led to a structured series of instruments including keeping records of data breaches, subject access requests, meetings, training sessions and policy decisions, together leading to a privacy culture across the company.

There are always new challenges ahead, for example, the yet to be finalised EU e-Privacy Regulation and digesting new policy initiatives from the ICO, such as the recent guidance on the use of cookies.

As with any business, Channel 4 needs to keep on making programmes to attract viewers and advertisers while complying with the data protection law in a way which enables the company to flourish into the future.

INFORMATION

Tamara Ballard spoke at the European Data Protection Summit on 3 June in London. See www.channel4.com/

Agreement struck between ICO and Facebook

On 30 October Facebook agreed to pay the £500,000 fine imposed by the ICO in 2018 for suspected failings related to compliance with the UK data protection principles covering lawful processing of data and data security.

As part of this agreement, Facebook and the ICO have agreed to withdraw their respective appeals. Facebook has agreed to pay the fine but has made no admission of liability in relation to the Monetary Penalty Notice. The fine is paid to HM Treasury's consolidated fund.

The agreement enables Facebook to retain documents disclosed by the ICO during the appeal for other purposes, including furthering its own investigation into issues around Cambridge Analytica. Parts of this investigation had previously been put on hold at the ICO's direction and can now resume, the ICO says.

James Dipple-Johnstone, Deputy Commissioner, said: "The ICO welcomes the agreement reached with Facebook for the withdrawal of their appeal against our Monetary Penalty Notice and agreement to pay the fine. The ICO's main concern was that UK citizen data was exposed to a serious risk of harm. Protection of personal information and personal privacy is of fundamental importance, not only for the rights of individuals, but also as we now know, for the preservation of a strong democracy. We are pleased to hear that Facebook has taken, and will continue to take, significant steps to comply with the fundamental principles of data protection. With this strong commitment to protecting people's personal information and privacy, we expect that Facebook will be able to move forward and learn from the events of this case."

Harry Kinmonth, Director and Associate General Counsel, Facebook said: "We are pleased to have reached a settlement with the ICO. As we have said before, we wish we had done more to investigate claims about Cambridge Analytica in 2015. We made major changes to our platform back then, significantly restricting the information which app developers could access. Protecting people's information and privacy is a top priority for Facebook, and we are continuing to build new controls to help people protect and manage their information. The ICO has stated that it has not discovered evidence that the data of Facebook users in the EU was transferred to Cambridge Analytica by Dr Kogan. However, we look forward to continuing to cooperate with the ICO's wider and ongoing investigation into the use of data analytics for political purposes."

• *See ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/10/statement-on-an-agreement-reached-between-facebook-and-the-ico/*

Immigration exemption in UK Act appealed

The High Court has dismissed the judicial review challenge to the Home Office regarding the 'immigration exemption' contained in the Data Protection Act 2018. The Open Rights Group and the3million who are behind the challenge say they are disappointed by the judgement and have applied for permission to appeal.

The Open Rights Group and the3million still believe that the immigration exemption in the Data Protection Act 2018 as it stands breaches fundamental rights. "It is a blunt instrument, poorly defined and ripe for abuse. Access to data is key to an accountable system, to correct errors that occur at an alarming rate in the immigration system," they say.

This exemption means that applicants cannot correct errors in their personal data which may prove decisive in immigration decisions. The government has used its discretion in interpreting the GDPR in response to 60% of its immigration-related data requests since the beginning of 2019, The Open Rights Group says.

The exemption is a deviation from the GDPR which may have an impact on any UK adequacy assessment.

• *See www.openrightsgroup.org/press/releases/2019/open-rights-group-and-the3million-seek-to-appeal-immigration-exemption-judgment*

events diary

Balancing privacy with biometric techniques used in a commercial context
29 January 2020
Macquarie Group, London
The objective of this Roundtable is for companies to exchange experience on how they are implementing and using biometric techniques in different scenarios, and their plans to use them in the future.
See www.privacylaws.com/biometric

Germany's data protection law: Trends, opportunities and conflicts
March 2020 (date to be confirmed)
Covington & Burling, London
Speakers include Alexander Filip, Head of Department, Bavarian Data Protection Authority and Covington & Burling lawyers based in Germany
See www.privacylaws.com/events

PL&B's 33rd Annual International Conference
29 June to 1 July 2020
St. John's College, Cambridge
This residential conference is an opportunity to enjoy a unique friendly summer-school atmosphere while mingling with a group of Data Protection Commissioners, privacy managers, specialist lawyers and academics from many countries.

Held at the beautiful St John's College, Cambridge, participants will enjoy the excellent facilities at the conference centre. Come and experience a classic Cambridge college and walk across the Bridge of Sighs over the River Cam.

This event qualifies for up to 18 SRA CPD hours and up to 12 CPE credits.
See www.privacylaws.com/ac

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 and events. You can then click straight through from the search results into the PDF documents.

3. Electronic Version
We will email you the PDF edition which you can also access 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 in Data Protection, Freedom of Information and related laws.

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

7. Events Documentation
Access UK events documentation such as *PL&B 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.

privacylaws.com/reports

"*PL&B* has been a data protection stalwart throughout my privacy career. Its publications continue to inform and challenge practitioners in the UK and around the world."

Simon McDougall, Executive Director – Technology and Innovation, ICO

International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 33rd year. Comprehensive global news, currently on 165+ 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.