Bird & Bird

UK & EU Data Protection Bulletin: June 2021

Welcome to your monthly newsletter from Bird & Bird's UK Data Protection team

In this month's newsletter, we bring you the following updates:

United Kingdom

ICO

UK Cases

EU

EDPB

ECHRT Cases

UK Enforcement

ICO Enforcement

United Kingdom

Information Commissioner's Office (ICO)

Date	Description
18 May	**Data Sharing Code of Practice – laid before Parliament on 18 May** The new Data Sharing Code of Practice published by the UK Information Commissioner's Office ("**ICO**") was laid before Parliament on 18 May 2021 and will come into force after 40 sitting days of Parliament. It replaces the ICO's first Data Sharing Code which was published in 2011 and required updating to reflect the requirements of the UK General Data Protection Regulation ("**UK GDPR**") and Data Protection Act 2018 ("**DPA 2018**"), as well as the enormous changes in the types and amounts of personal data collected by organisations and in the technology used to store and share such data in the intervening period. It is important to note that the Code focusses on providing guidance for the sharing of personal data between controllers, whether that is as part of routine data sharing, a one-off transfer or as part of a data pooling arrangement. Controller to processor sharing is out of scope of the Code. The Code also does not apply to sharing of personal data internally within an organisation. It is a statutory code of practice and the Commissioner must take the Code into account when considering whether an organisation has complied with its data protection obligations when sharing data, in particular as regards questions of fairness, lawfulness, transparency and accountability under the UK GDPR and the DPA 2018, as well as when considering use of her enforcement powers. If the Code is not followed, it may be more difficult for an organisation to demonstrate that its data sharing is fair, lawful and accountable and complies with the UK GDPR and the DPA 2018. The Code also contains some optional good practice recommendations. The Code flags that, when sharing personal data, the following key principles apply: • The accountability principle means that an organisation is responsible for its compliance and must be able to demonstrate that compliance. • The personal data must be shared fairly and transparently. • At least one lawful basis for sharing data must be identified before any disclosure takes place. • The personal data must be processed securely, with appropriate organisational and technical measures taken. • The Code also recommends that, when sharing personal data, organisations take the following practical steps: - involve the organisation's data protection officer in the proposed data sharing arrangement; - carry out a Data Protection Impact Assessment as a matter of good practice even if not required; - document the data sharing in a Record of Processing Activities; and • put a data sharing agreement in place to help demonstrate accountability - this agreement should be reviewed regularly and should include the parties, the purposes of sharing (and the specific intended benefits), the details of all organisations involved (including contact details for a privacy contact), what data will be shared ('data specification'), the lawful basis of processing/sharing, and any

Date	Description
	relevant legal powers – including copies of any consent, procedures for data subject rights, security standards and information governance. Finally, the Code contains specific guidance on certain key areas of data sharing e.g. following mergers and acquisitions, database and list transfers, sharing of children's personal data and data sharing in an emergency.
28 May	**ICO seeking views on the first chapter of its Anonymisation Guidance** The ICO has published the first draft chapter of its Anonymisation, Pseudonymisation and Privacy enhancing technologies draft guidance for consultation. This chapter examines the legal, policy and governance issues around the application of anonymisation and pseudonymisation in the context of data protection law. A copy of the chapter can be found here. The consultation closes on 28 November. Further chapters will be released over the coming months and will include: • Identifiability – outlining approaches such as the spectrum of identifiability and their application in data sharing scenarios, including guidance on managing re-identification risk, covering concepts such as the 'reasonably likely' and 'motivated intruder' tests; • Guidance on pseudonymisation techniques and best practices; • Accountability and governance requirements in the context of anonymisation and pseudonymisation, including data protection by design and DPIAs; • Anonymisation and research - how anonymisation and pseudonymisation apply in the context of research; • Guidance on privacy enhancing technologies (PETs) and their role in safe data sharing; • Technological solutions – exploring possible options and best practices for implementation; and • Data sharing options and case studies.

UK Cases

Date	Cases
2 March	**Mohammed Belal Uddin v The Information Commissioner (EA/2020/0353/GDPR)** The First-tier Tribunal (General Regulatory Chamber) ("Tribunal") struck out Mr Uddin's application under sections 166(2) and 166(3) Data Protection Act 2018 ("DPA 2018"), because the DPA 2018 does not provide a right of appeal against the substantive outcome of a complaint investigation. Rather, the Tribunal is limited to issuing orders concerning whether the Information Commissioner has: (a) taken appropriate steps to address a complaint; (b) informed the complainant of progress of the complaint; and (c) informed the complainant of the outcome of the complaint. Mr Uddin made a complaint to the Commissioner in June 2019 in relation to the way his employer, BGC Technology International Limited ("**BGC**") processed his personal data in the context of work email communications with colleagues. The Commissioner took various steps to respond to the complaint, including allocating a case reference number and an ICO case officer, who sought further information from both Mr Uddin and BGC. The case officer ultimately responded to Mr Uddin, stating that it was the case officer's belief that BGC had complied with its data protection obligations and no further action would be required. Mr Uddin requested a case review, which a reviewing officer undertook and concluded that the previous case officer had handled the matter appropriately. Upon further correspondence with Mr Uddin, the Commissioner wrote to Mr Uddin and explained that these recent queries did not raise any additional issues, and that the matter would be considered closed. In summary, given that a section 166 DPA 2018 application relates to procedural concerns, the Tribunal was not concerned with the strengths and merits of the underlying complaint. Case law has also established that "appropriate steps to respond to a complaint" reflects exactly that, and not the power to resolve the complaint. For these reasons, the Tribunal struck out Mr Uddin's application.
12 March	**Ticketmaster UK Ltd v Information Commissioner (EA/2020/0359/FP)** This case relates to an appeal made by Ticketmaster against a penalty notice of £1.5million issued by the ICO in November 2020 relating to a data breach linked to a chatbot used on its website and provided to Ticketmaster by a third party, Inbenta Technologies Limited. The grounds of appeal include arguments that Ticketmaster did not breach its obligations under Articles 5(1)(f) and 32 of the GDPR, that the security incident resulted from an unforeseen and criminal attack on Inbenta and Inbenta's failure to maintain appropriate security or alternatively that the penalty imposed was excessive. However, given the ongoing proceedings in the High Court which arise out of the same incident (Collins & Others v Ticketmaster UK Ltd (BL-2019-LIV-000007) which have been brought by some 795 Ticketmaster customers, the Tribunal decided to stay the appeal proceedings until 28 days after the High Court judgement had been delivered.

Date	Cases
May	**Representative Action being brought against TikTok for breach of GPDR** A class action has been filed in the UK High Court against TikTok, alleging breaches of UK and EU data protection law in respect of the way in which the video-sharing app collects and uses personal data of children. The claim has been brought as a "representative action" under Civil Procedure Rule 19.6, the same mechanism used by Richard Lloyd in his well-publicised claim against Google. To bring such an action, a claimant must show that all those represented have the "same interest" in the claim. It has been brought against two ByteDance companies (Bytedance owns TikTok) and Musical.ly, TikTok's predecessor. Officially it has been brought by an anonymised 12 year old child with the backing of England's former Children's Commissioner, Anne Longfield, who is acting as the child's "litigation friend". As a representative action, it is an opt-out claim, meaning all under 13-year old TikTok users in the UK, and all under-16 year old users in the European Economic Area, are represented unless they choose not to be. The claim focusses on complaints that TikTok collects children's personal information, including phone numbers, videos, exact location and biometric data, and allegations that this data is taken without sufficient warning, transparency or the necessary consent, and without children or parents knowing what is being done with that information. It is alleged that this practice breaches the UK DPA 2018, the EU GDPR and the UK GDPR (post-Brexit) in a number of ways, namely: • Having inadequate measures in place to prevent children from downloading and/or using TikTok; • Having inadequate messaging to explain which data was collected and how this was being further processed to facilitate informed decision-making by users; • Failing to provide the user with adequate transparency about the nature and extent of the processing of their data; • Failing to acquire the relevant and necessary consent of the children's parents or guardians, or any effective consent; and/or • Failing to have any effective contractual basis or legitimate interest to process the personal data in this manner. The class action is being funded by a venture capital outfit, who will take a share of any damages pot ultimately awarded. The claimants have suggested to the press that damages of several thousand pounds should be paid to each child represented. This seems high relative to analogous claims to date - for example, each claimant in Lloyd v Google is claiming only £750 damages for loss of control of personal data. Damages were pitched at this level in the Lloyd case to enable the claimants to meet the "same interest" test under CPR 19.6 - in essence, they abandoned any claim for damages for individual distress suffered (where differences could exist) and instead claimed a uniform sum for loss of control alone. If the claimants in the TikTok case wish to use the 19.6 mechanism similarly, it will be interesting to see if they do in fact pursue this higher level of damages. The claim is currently stayed pending the Supreme Court's decision in Lloyd v Google, expected later this year. A similar claim against TikTok has also recently been filed in the Amsterdam Court, also alleging breaches of the EU GDPR in relation to collection of children's personal data. That claim is brought by a purpose-built representative body, a parents group called the Market Information Research Foundation (SOMI), which charges parents a low sum to join the claim register, which enables them to fund the litigation. SOMI has had 64,000 parents sign up to the claim, although it claims to represent, on an opt-out basis, over one million children. Depending on their age, each child is claiming between €500-2000, amounting to total damages claimed of €1.4 billion. Given the stay of the UK claim, it may be that an outcome is reached in the Dutch claim sooner.

Date	Cases
26 May	**R (Open Rights Group and the3million) v Secretary of State for the Home Department and Others [2021] EWCA Civ 800** On May 26, 2021, the Court of Appeal handed down its judgment in the case of R (Open Rights Group and the3million) v Secretary of State for the Home Department and Others. Finding in favour of the claimant, the Court of Appeal held that the "immigration exemption" in Schedule 2 paragraph 4 UK 2018 Data Protection Act's ("DPA 2018") is non-compliant with GDPR (which was integrated into UK law by virtue of the European Union (Withdrawal) Act 2018). The DPA's immigration exemption exempts persons who process personal data for purposes related to immigration control from the data subject rights guaranteed by the EU General Data Protection Regulation ("GDPR") to the extent that complying with those provisions would prejudice such purposes. The GDPR allows jurisdictions to incorporate exemptions from certain GDPR obligations in their implementing legislation. Such exemptions must be necessary and proportionate in a democratic society to pursue the relevant objective. Art 23(2) provides that any exemption must include provisions relating to its purpose, scope and safeguards. The Court at first instance upheld the exemption, however the Court of Appeal overturned this decision, finding that while the exemption addresses an important public interest, it does not include the necessary limitations and safeguards to protect the fundamental rights and freedoms of individuals. The Court's finding is consistent with the EDPB's criticism of the UK's immigration exemption and could raise further questions regarding the Commission's imminent determinaton as whether or not the UK has an adequate data protection regime (for data transfer purposes).
28 May	**Mr Baldo Sanso Rondon and LexisNexis Risk Solutions UK Limited [2021] EWHC 1427 (QB)** This recent High Court judgment confirms the limited role played by data protection representatives appointed in accordance with Article 27 GDPR and finds that such representatives cannot be held liable for the action of their foreign data controllers. In this case, the claimant, an Italian based businessman, argued that the UK based representative(Lexis Nexis Risk Solutions UK Limited) was responsible for alleged breaches of GDPR by World Compliance Inc, the US based data controller it represents in respect of the profiles it maintained about the claimant in its financial screening database. In particular, the claimant sought an order requiring the representative to erase the claimant's personal data (under S167 DPA 2018), notify each recipient to whom the data had been disclosed (under Art 19 GDPR) and compensate the claimant (under Art 82 GDPR). By way of reminder, Article 27 GDPR requires the controller or processor to designate a representative in the EU where Article 3(2) GDPR applies, namely where the organisation is not established in the EU but (i) offers goods or services to individuals in the EU or (ii) monitors the behaviour of individuals in the EU. Similar provisions relating to the appointment of a UK representative now exist under the UK GDPR, in effect following the end of the Brexit transition period. However as the claim was made in August 2020, the case was made in respect of the EU GDPR. The case centred around the interpretation of Art 27.4 and 27.5 GDPR (with the parties agreeing that the GDPR in general and Art 3.2 and Art 27 GDPR applied) and in particular, considered Recital 80 GDPR, the DPA 2018 and the EDPB Guidelines 3/2018 (Territorial Scope) on this point as well as examining how representatives were treated in other EU instruments. As there was little ICO guidance, the representative had also written to the ICO on 9 March 2021 inviting them to express a view on the interpretative question at issue.

Date	Cases
	Although the ICO did not seek to intervene in the proceedings, it did share the representative's view that the role of an Art 27 representative "is limited to that of conduit of communications between the overseas entity and the ICO or relevant data subjects…and the ICO is not seeking an interpretation of Art 27 that allows representatives to be held directly liable should a controller or processor they represent fail in their data protection obligations." After reviewing the various background materials as well as giving weight to the ICO's practical view, the judge agreed with the representative and struck out the claimant's arguments after finding "no basis in law" for the claim. However the judge did comment that the role of a representative is 'a considerably fuller role that a mere postbox 'to be addressed"…The role is an enriched one, active rather than passive…The job focusses on providing local transparency and availability to data subjects and local regulatory co-operation." We agreed that this was the only sensible outcome – a judgment that representatives can be held liable would act as a major disincentive for organisations to take on that role, which of course is central to the GDPR framework for non-EU established companies. Bird & Bird Privacy Solutions Team can provide EU & UK Representative Services: For more information, see here.

EU

EDPB

Date	Description
19 May	**Opinion 16/2021 on the draft decision of the Belgian Supervisory Authority regarding the "EU Data Protection Code of Conduct for Cloud Service Providers" submitted by Scope Europe** On 20 May 2021, the Belgian Data Protection Authority ("BDPA") has approved the first transnational code of conduct for cloud services ("EU Cloud CoC") to be adopted within the EU since the entry into force of the General Data Protection Regulation (EU) 2016/679 ("GDPR"). The EU Cloud CoC aims to establish good data protection practices for cloud service providers and intends to contribute to a better protection of personal data processed in the cloud. Several large industry players have endorsed the EU Cloud CoC. Pursuant to Article 40(1) GDPR, Member States, supervisory authorities, the European Data Protection Board as well as the European Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR. The purpose of the EU Cloud CoC is to do just that, namely to create a baseline for practical implementation of the GDPR for cloud providers of all types (IaaS, PaaS or SaaS). This includes the Article 28(1) and (5) GDPR requirement for processors to implement sufficient guarantees around their technical and organisation means. As such, processors can use the adherence to the EU Cloud CoC to demonstrate that such means have been implemented. Furthermore, the EU Cloud CoC provides guidance (both for controllers as for processor) regarding often recurring issues, such as for example audit rights, the deletion and return of personal data, technical and organisational security measures, transparency requirements or liability. It should be noted, however, that the EU Cloud CoC is only applicable to processors offering cloud services, and therefore not in a B2C context or to any processing activities for which the cloud service provider may act as a controller. Neither does the EU Cloud CoC constitute an international transfer mechanism under Article 46(2)(e) GDPR. Since Articles 40 and 41 GDPR require approved codes of conduct to be monitored, the body accredited by the BDPA for monitoring compliance with the provisions of the EU Cloud CoC, is SCOPE Europe. As part of the approval process, the European Protection Board provided a favourable opinion regarding the EU Cloud CoC. You may also be interested in the BDPA's approval decision, the accreditation decision of Scope Europe and the BDPA's press release.
19 May	**Recommendations issued by EDPB on storage of credit card data after payment made for goods and/or services online** On 19 May 2021, the EDPB adopted its Recommendations on the legal basis for the storage of credit card data for the sole purpose of facilitating further online transactions. On the question of whether online retailers are allowed to keep a customer's credit card details after a purchase has been made (in case the customer wants to make another purchase in the future and to save them having to re-enter their card details, which might facilitate

further purchases), the EDPB has concluded that consent under Article 6(1)(a) of the UK GDPR "appears to be the sole appropriate legal basis" for the storage of these details.

Unsurprisingly, the EDPB expressly ruled out the possibility of reliance on the following heads under Article 6 of the UK GDPR: necessity for compliance with a legal obligation, protection of the vital interests of a natural person, and performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Also unsurprisingly, the EDPB ruled out reliance on necessity for the performance of a contract to justify the keeping of the credit card details, on the basis that the provision of these details by the customer was clearly necessary for the completed online purchase but keeping them for the purpose of facilitating a *potential* new transaction is not necessary for the transaction just concluded.

More interesting was the EDPB's view on reliance on legitimate interests as the legal basis for the processing - the EDPB did not reject legitimate interests arguments out of hand (see sections 7-9 of the Recommendations) but ultimately took the view that, in this specific context, under the balancing test to be performed to weigh up the controller's legitimate interests against the individual's interests and fundamental rights and freedoms, the latter would prevail and the legitimate interests basis could not be relied upon. This was justified mainly on the grounds that the nature of the data involved (i.e. credit card details), like other financial data, are of a "highly personal nature" and that serious harm could result were such details not to be adequately protected ("their violation clearly involves serious impacts on the data subject's daily life"). The EDPB also highlighted another important element of the balancing test, namely that when a purchaser provides his/her credit card details to make an online purchase, he/she does not reasonably expect those details to be stored for longer than necessary to complete the current purchase. Therefore, as noted above, the EDPB concluded that an individual's specific consent should be obtained for storing of his/her credit card details after a purchase – both to address security risks given the nature of the data and to allow the individual to be able actively to decide what happens to his/her data.

The EDPB sets out the requirements for this consent, in line with its previous Guidelines on Consent: (i) the consent "cannot be presumed by the simple fact that he/she concluded one, or several, isolated transactions"; (ii) it must be free, specific, informed and unambiguous; (iii) it should be requested in a user-friendly way and delivered by a clear affirmative action (such as via a checkbox, which should not be pre-ticked) on the page where the credit card details are collected; (iv) it must not be bundled with any general consent given to the retailer's terms of business and/or privacy policy, and not made a condition to the completion of the purchase; and (v) it should also be easily withdrawn at any time should the individual so wish. Given these new recommendations from the EDPB, we suggest that retailers revisit their transactional websites to ensure that consent is sought for any storage of credit cards details after a purchase.

See also our recent news alert on these Guidelines: https://www.twobirds.com/en/news/articles/2021/uk/edpb-recommends-collecting-consent-to-store-credit-card-details-for-future-transactions

EctHR

Date	Description
June 2021	**ECtHR rules UK surveillance violated ECHR** The European Court of Human Rights Grand Chamber has now delivered its twin bulk surveillance judgments in *Big Brother Watch* and *Centrum för Rättvisa*. The Grand Chamber held that neither the former UK regime (under the Regulation of Investigatory Powers Act 2000) nor the Swedish regime considered in *Rättvisa* complied with the European Convention on Human Rights. However, it reached that conclusion on relatively narrow grounds. For the UK, the practical issue now is whether the decisions cast any doubt on the current Investigatory Powers Act 2016. The high level takeaway is that the judgments lay down a revised set of criteria by which to assess bulk surveillance regimes against the requirements of the Convention, but do not forbid them as such. The Court concluded that a decision to operate a bulk interception regime continues to be one that a Contracting State can make. A State's freedom of choice in how to operate such a regime is, however, more constrained. **Minimum criteria** The Court laid down eight minimum criteria to be considered in deciding whether a bulk surveillance regime passes the Convention's 'in accordance with the law' and 'necessity' tests. The criteria are whether the domestic framework clearly defines: 1 the grounds on which bulk interception may be authorised; 2 the circumstances in which an individual's communications may be intercepted; 3 the procedure to be followed for granting authorisation; 4 the procedures to be followed for selecting, examining and using intercept material; 5 the precautions to be taken when communicating the material to other parties; 6 the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;

7 the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;

8 the procedures for independent ex post facto review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.

The Court will make an 'overall assessment' of the bulk interception regime, in which shortcomings in some areas may be compensated by safeguards in others. The Court may also take into account factors beyond the eight minimum criteria, such as provisions for notification of surveillance subjects.

It is unclear to what extent these minimum criteria represent threshold conditions to be surmounted, and to what extent they are only factors to be taken into account. This underlying ambiguity was the subject of trenchant criticism in a separate Opinion of Judge Pinto de Albuquerque.

Content versus metadata (communications data)

Significantly, the Court was not persuaded that the acquisition of communications data through bulk interception is necessarily less intrusive than the acquisition of content. Interception, retention and searching of communications data should be analysed by reference to the same safeguards as those applicable to content.

That said, the Court observed that while the interception of related communications data would normally be authorised at the same time the interception of content is authorised, once obtained they could permissibly be treated differently by the intelligence services. As long as the relevant safeguards were in place, the legal provisions governing treatment of communications data did not necessarily have to be identical in every respect to those governing the treatment of content.

End-to-end safeguards

Building on its eight minimum criteria. the ECtHR laid down the "fundamental safeguards" that would be the cornerstone of an Article 8-compliant bulk interception regime.

These were articulated in the context of the particular model presented to the court (collection, filtering to discard unwanted material, automated application of selectors and search queries, manual queries by analysts, examination by analysts, subsequent retention and use), which the Court characterised as involving increasing interferences with privacy as the process progressed.

(This model already feels rather old-fashioned, given the sophisticated pattern-matching and other techniques that are capable of being applied to the analysis of, in particular, bulk communications data.)

The court laid down that the process must be subject to end-to-end safeguards, meaning that:

- At each stage of the process an assessment must be made of the necessity and proportionality of the measures being taken.
- Bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined

- The operation should be subject to supervision and independent *ex post facto* review

The Court commented that the importance of supervision and review is amplified compared with targeted interception because of the inherent risk of abuse and the legitimate need for secrecy.

Drilling down further, the Court stipulated that:

- The independent authorising body should be informed of both the purpose of the interception and the bearers or communication routes likely to be intercepted.
- The authorisation should at the very least identify the types or categories of selectors to be used.
- Enhanced safeguards should be in place for strong selectors linked to identifiable individuals. These include scrupulous recording of the justification for their use and a separate, objective process of prior internal authorisation.
- Each stage of the bulk interception process should be subject to supervision by an independent authority, sufficiently robust to keep the interference with Art 8 rights to what is "necessary in a democratic society". Detailed records should be kept by the intelligence services at each stage.
- An effective remedy should be available to anyone who suspects that his or her communications have been intercepted by the intelligence services, either to challenge the lawfulness of the suspected interception or the Convention compliance of the interception regime. A remedy that does not depend on notification to the interception subject can be effective. But it must then be before an independent body that ensures fairness of the proceedings, offering, in so far as possible, an adversarial process. Decisions shall be reasoned and legally binding as to, inter alia, ceasing unlawful interception and destroying unlawfully obtained and/or stored intercept material.

The court also provided guidance on sharing intercept material with agencies in other countries.

The Court will conduct a global assessment of the operation of the regime, focusing primarily on whether the domestic legal framework contains sufficient guarantees against abuse, and whether the process is subject to end-to-end safeguards.

In doing so, the Court will have regard to the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of any evidence of actual abuse.

The Court's decision on RIPA

In *BBW* the UK's now superseded Regulation of Investigatory Powers Act 2000 (RIPA) regime was under challenge. As in the Chamber judgment in 2018 the Grand Chamber found the UK regime wanting, and on broadly similar grounds. The specific points on which it found the RIPA regime deficient were:

- Lack of independent authorisation at the outset
- Lack of provision for oversight of categories of selectors at the point of authorisation; lack of provision for enhanced safeguards for use of strong selectors linked to identifiable individuals
- Insufficiently precise nature of the Secretary of State certificate as to descriptions of material necessary to be examined

'Selectors' refers to operators such as search terms, which might be applied in near-real time or after a delay. They might be specific 'strong' selectors such as e-mail addresses, or complex queries constructed from multiple single terms.

These criticisms applied to both content and communications data acquired alongside content: so-called Related Communications Data (RCD).

- Longer storage periods for RCD ("several months") were not evident in the Interception Code. They should be included in legislative or other general measures.

Specific criticisms were directed to the treatment of journalistic material, which the Court found breached Article 10:

- There was no requirement for a judge or similar to decide whether use of selectors or search terms known to be connected to a journalist was justified by an overriding requirement in the public interest; or whether a less intrusive measure might have sufficed [456];
- Nor was there any provision for similar authorisation of continued storage and examination of confidential journalistic material once a connection to a journalist became known. [457]

Independent prior authorisation

The main concrete point of difference from the Chamber judgment is probably the Grand Chamber's greater emphasis on prior independent authorisation. That, in the form of Judicial Commissioner approval of the Secretary of State's decision to issue a warrant, is now a feature of the Investigatory Powers Act 2016 which superseded RIPA.

The Swedish regime considered in *Rättvisa* did feature prior authorisation by an independent Foreign Intelligence Court. Even so, the Grand Chamber found certain shortcomings that were not compensated for by other safeguards.

Implications for the Investigatory Powers Act 2016

It is difficult to predict specific implications for the IP Act. This is due to the Court's holistic, multifactorial approach to fundamental rights compliance. However, the Act does tick some important boxes, notably the "double lock" system of approval of bulk warrants by an independent Judicial Commissioner introduced after the end of the RIPA regime.

The IP Act in some respects provides stronger safeguards than those that fell short in *Rättvisa* – the UK Investigatory Powers Tribunal was held up as an example of what was possible in the area of *ex post facto* review.

On the other hand, the Swedish regime provided for mandatory presence of a privacy protection representative at Foreign Intelligence Court sessions. That was identified as a relevant safeguard to be weighed against the fact that the Court had never held a public hearing and that all its decisions were confidential. There is no provision in the IP Act for a privacy protection representative to make submissions in the bulk warrant approval process.

As to publicising bulk warrant approval decisions, in his April 2018 Advisory Notice the Investigatory Powers Commissioner said:

"The Judicial Commissioners will consider making any decisions on approvals public, subject to any statutory limitations and necessary redactions."

No regular practice of publishing decisions has emerged. The Commissioner's Annual Report has made occasional reference to approvals.

As for the double-lock procedure itself, in April 2018 the Commissioner issued an Advisory Notice stating that the Judicial Commissioners would not apply the relatively hands-off 'Wednesbury reasonableness' test, but instead the judicial review test applied by the domestic courts when considering interferences with fundamental rights. That would be taken into account in any assessment of the level of scrutiny applied to warrants.

Bulk communications data acquisition

An area of the IP Act that is likely to attract attention is the IP Act's bulk communications data acquisition warrant. This is the successor to S.94 of the Telecommunications Act 1984, which the government admitted in November 2015 had been used for bulk acquisition of communications data from communications service providers.

Unlike bulk interception under RIPA or the IP Act, the bulk communications acquisition warrant is domestic rather than focused on foreign intelligence purposes. Given the various references in the *BBW* and *Rättvisa* judgments to bulk interception being primarily used for foreign intelligence, and the acknowledgment that bulk communications data should not be regarded as less sensitive than content, the Convention compliance of a domestic bulk acquisition regime may come to be considered in the future.

Journalistic privilege

Although the IP Act contains stronger protections for journalistic material than did RIPA, it may be questioned whether those, at least of themselves, are sufficient to meet the criticisms contained in the two ECtHR judgments.

End-to-end safeguards under the IP Act

Returning to the central theme of the Grand Chamber's stipulated safeguards, does the IP Act provide sufficient end-to-end safeguards over the bulk interception process?

Since the IP Act does not spell out whether, and if so how, end to end oversight must be applied to all stages of the bulk interception process, more may need to be done to fill that gap. That may not necessarily require amendment of the Act, although it would be preferable if any steps taken unambiguously formed part of the legal regime.

A published explanation of how closely the Judicial Commissioners oversee the various selection, searching and other analytical processes would assist. An IPCO Advisory Notice could usefully spell out the IPC's understanding of the relevant requirements of the Act; and explain how that translates into practical oversight, as part of bulk warrant approval or otherwise, of the end-to-end stages involved in bulk interception and other bulk powers.

https://www.cyberleagle.com/2021/06/big-brother-watchrattvisa.html

UK Enforcement

UK ICO Enforcement

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
18 May 2021	Tested.me Ltd ("**TML**")	Monetary penalty of £ 8.000	The ICO imposed a monetary penalty on contact-tracing service, TML, for not having the necessary valid consent in relation to sending 83,904 direct marketing messages to its subscribers. TML provides digital "track-and-trace" services to businesses for contact-tracing purposes. TML does this by issuing QR codes which individuals scan when they enter business premises, after which their track-and-trace details are provided automatically. These details included name, time and date of visit, contact information and the existence of an TML app profile if applicable. Following a complaint by an individual regarding the receipt of an unsolicited marketing email in November 2020, the ICO investigated and found that TML promoted its own Digital Health Passport App to almost 84,000 people who had used their QR code technology. The complainant stated that they did not consent to this email, nor did they believe they had any relationship with TML. Subsequent investigations found that the individual may have signed up to marketing emails after completing a "Visitors Registration Form" (the "**Form**"), into which they had entered their track and trace details. This Form included consent wording which stated that the individual agreed to receiving marketing communications from the venue, its alliance and TML (if the box was ticked). TML also experienced some technical and administrative difficulties in processing when individuals had chosen to opt out. The ICO ultimately found that TML had not acquired valid consent for sending the emails because the consent was not: • **Informed**, as TML did not provide enough information about who they were, what they did or what their exact relationship with the venue in question was, nor did TML provide a link to its Privacy Policy in the Form. • **Specific or freely given,** because the Form bundled consent for several purposes, and gave individuals no choice to select a method of marketing communication, i.e. by email or phone. In deciding the amount of the fine, the ICO considered, among other things, the content of the Privacy Policy and other documentation as well as the provision of the data protection training for staff.

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
20 May 2021	American Express Services Europe Limited ("**Amex**")	Monetary penalty of £90,000	The ICO has fined Amex £90,000 for unlawfully sending more than 4 million direct marketing emails between June 2018 and May 2019 to subscribers in the absence of adequate consent. The ICO launched an investigation after it received three complaints from Amex customers who were receiving marketing emails after having opted out. These emails described how customers could utilise reward programmes by shopping online with Amex and also encouraged customers to download the Amex app, to get the most benefit from using their Amex cards. Amex classified these emails as "servicing" rather than "marketing" emails. In Amex's view, marketing emails were those which advertised additional products or services, or were related to renewing contracts close to termination. Amex stated that "we feel that Card Members would be at a disadvantage if they were not aware of these campaigns and promotional periods". However, the ICO disagreed with Amex and concluded that the emails could not be classified as servicing messages. The ICO argued that the emails clearly contained marketing material because they aimed to persuade and encourage customers to use their Amex cards, which benefitted Amex financially. Moreover, the ICO found that Amex did not rely on valid consent to send the direct marketing messages because consent was not: • **freely given**, as it was conditional to receiving Amex's services (where consent was not necessary for contractual performance of Amex) and customers were not able to withdraw consent. • **informed,** because the legal and contractual requirements were bundled with the overall terms and conditions. In calculating the fine, the ICO considered, among other things, that: (i) there was a deliberate contravention of Regulation 22 PECR because it was a deliberate action for financial or personal gain; (ii) Amex did not have internal procedures which were compliant with PECR; (iii) Amex did not consult the ICO Guidance on Direct Marketing; and (iv) Amex had failed to review its marketing model in light of complaints regarding the same.
3 June 2021	The Conservative Party MPN (the "**Party**")	Monetary penalty of £10,000	The ICO has fined the Party £10,000 after it sent 51 marketing emails to individuals who had not validly consented to receiving them. Boris Johnson became Prime Minister on 23 July 2019, after which the Party ran an eight-day email marketing campaign in the name of the Prime Minister. The emails promoted the Party's political

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
			agenda in relation to Brexit, investment in the NHS, housing and crime. After having received a high number of complaints within a short space of time, the ICO launched an investigation. The ICO found that the Party had contravened PECR because valid consent had not been obtained in respect of any of the 51 complainants. In some situations, the Party could not provide evidence of any consent at all, and in others, the Party admitted that it had wrongly failed to unsubscribe individuals from direct marketing due to administrative errors. Generally, consent was not freely given, specific or informed. The ICO found the contravention particularly serious because: (i) the Party has sent such a large number of marketing emails in total (1 million in 8 days); (ii) the Party did not have records of consent for 549,030 recipients; and (iii) the Party did not have any relevant written policies.

Other recent articles

Joint Statement from the ICO and CMA: https://www.twobirds.com/en/news/articles/2021/uk/when-competition-law-and-data-protection-overlap

European Commission publishes landmark Artificial Intelligence regulatory package (twobirds.com)

Replacement Standard Contractual Clauses (SCCs): European Commission publishes final text

The other SCCs - New Art. 28 SCCs published

Webinars

New SCCs and Art 28 GDPR terms: where do we start?

For information on the international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses, our offices, our members and partners, regulatory information, privacy, complaints procedure and the use of e-mail see www.twobirds.com/LN . Bird & Bird LLP, a limited liability partnership, registered in England and Wales with registered number OC340318, with its registered office and principal place of business at 12 New Fetter Lane, London EC4A 1JP, is authorised and regulated by the Solicitors Regulation Authority, whose professional rules and code may be found at www.sra.org.uk/handbook/ . A list of members of Bird & Bird LLP and of any non-members who are designated as partners, being lawyers or other professionals with equivalent standing and qualifications, and of their respective professional qualifications, is open to inspection at its registered office. References in this document to "Bird & Bird", the "firm", "we" or "our" mean Bird & Bird LLP and the other affiliated and associated businesses authorised to carry the name "Bird & Bird" or one or more of Bird & Bird LLP and those affiliated or associated businesses as the context requires.

twobirds.com

Abu Dhabi & Amsterdam & Beijing & Berlin & Bratislava & Brussels & Budapest & Copenhagen & Dubai & Dusseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Luxembourg & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & San Francisco & Shanghai & Singapore & Stockholm & Sydney & Warsaw

The information given in this document concerning technical legal or professional subject matter is for guidance only and does not constitute legal or professional advice. Always consult a suitably qualified lawyer on any specific legal problem or matter. Bird & Bird assumes no responsibility for such information contained in this document and disclaims all liability in respect of such information.

This document is confidential. Bird & Bird is, unless otherwise stated, the owner of copyright of this document and its contents. No part of this document may be published, distributed, extracted, re-utilised, or reproduced in any material form.

Bird & Bird is an international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses.

Bird & Bird LLP is a limited liability partnership, registered in England and Wales with registered number OC340318 and is authorised and regulated by the Solicitors Regulation Authority. Its registered office and principal place of business is at 12 New Fetter Lane, London EC4A 1JP. A list of members of Bird & Bird LLP and of any non-members who are designated as partners, and of their respective professional qualifications, is open to inspection at that address.