XX

Investigations In England & Wales: Practitioners' Perspective

Michael Drury and Julian Hayes[1]

There is no dedicated, comprehensive cybersecurity law as such in England and Wales. Rather, there is a patchwork of statute-based laws, underpinned by the possibility of civil actions at common law. These laws criminalise unauthorised interference with computers (the Computer Misuse Act 1990 (CMA)); criminalise the interception of communications (Part 1 of the Investigatory Powers Act 2016 (IPA) and the Wireless Telegraphy Act 2006 (WTA)); impose obligations to protect personal data by the application of appropriate technical and organisational security measures (the United Kingdom General Data Protection Regulation (the UK GDPR), Data Protection Act 2018 (DPA), and Network and Information Systems Regulations 2018 (NISR)); and provide state agencies with the power lawfully to interfere with personal property (Part III of the Police Act 1997 (PA) and Intelligence Services Act 1994 (ISA)).

Computer Misuse Act 1990

The CMA, implementing the Budapest Convention on cybercrime,[2] is the principal criminal law deterrent to computer interference. Its basic criminal offence is committed where (1) a person causes a computer to perform any function with intent to secure access to any program or data held in any computer, or to enable any such access to be secured; (2) the access the person intends to secure or to enable is unauthorised; and (3) the person knows at the time when he or she causes the computer to perform the function, that this is the case.[3]

1 Michael Drury and Julian Hayes are partners at BCL Solicitors LLP.

2 https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

3 Section 1 of the CMA, carrying a maximum sentence of two years' imprisonment.

Securing access to a computer or a program encompasses many different actions. 'Computer' is not defined in the CMA.[4] Access is unauthorised if it is obtained by a person who is not entitled to control access to the program or data and is done without the consent of such a person.[5]

The CMA creates further offences where unauthorised access is sought with a view to committing other offences (e.g., theft or fraud);[6] or to impair the operation of a computer,[7] which would include the implanting of viruses or spyware and distributed denial-of-service (DDoS) attacks. The CMA also criminalises the obtaining, making, adapting, supplying or offering of articles for use in committing CMA offences.[8] The most serious offence under the CMA is committed if a person (1) does any authorised act in relation to a computer; (2) at the time of doing the act the person knows that it is unauthorised; (3) the act causes or creates a significant risk of serious damage of a material kind; and (4) the person intends to cause serious damage of a material kind or is reckless as to whether such damage is caused.[9] For the purposes of this offence, damage is of a 'material kind' if it is, for example, to the national security of any country.[10]

Investigatory Powers Act 2016

The IPA was introduced in response to heightened scrutiny of the surveillance activities of public authorities in the UK concerning the government's collection and use of communications and communications data. In essence, the IPA seeks to provide a comprehensive scheme for the use of investigatory powers by public authorities to obtain communications and communications data; undertake electronic surveillance more generally (including through 'hacking'); and access personal data held in large datasets. The IPA aims to ensure that the requirements of the Human Rights Act 1998 and the European Convention on Human Rights are met. Broadly speaking, these powers cover five areas of activity:

- interception warrants (specific and bulk);
- obtaining communications data (including bulk acquisition warrants);
- retention of communications data;
- equipment interference (including bulk equipment interference); and
- using bulk datasets.

A further overarching element is that a telecommunications operator[11] either based in the UK or outside the UK, can be mandated to take steps to give effect to a relevant authorisation by

4 In *DPP v. McKeown*; *DPP v. Jones* [1997] 2 Cr. App. R. 155 HL, Lord Hoffman defined a 'computer' as 'a device for storing, processing and retrieving information.' The Budapest Convention defines a 'computer system' as 'any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

5 Section 17(5) of the CMA.

6 Section 2 of the CMA, carrying a maximum sentence of five years' imprisonment.

7 Section 3 of the CMA, carrying a maximum sentence of 10 years' imprisonment.

8 Section 3A of the CMA, carrying a maximum sentence of two years' imprisonment.

9 Section 3ZA of the CMA, carrying a maximum sentence of life imprisonment.

10 Section 3ZA(2)(d).

11 Defined in section 261(10) of the IPA.

way of a technical capability notice (TCN)[12] (except in the case of retention of communications data or bulk datasets). When issuing a TCN, the Secretary of State must be satisfied as to its necessity and proportionality,[13] and approval must be sought from an independent Judicial Commissioner.[14]

Further, the IPA provides the framework for oversight for example by establishing the role of the Investigatory Powers Commissioner and the Investigatory Powers Tribunal.[15]

Wireless Telegraphy Act 2006

Where 'bugging' would not already be caught by the prohibition on unlawful interception contained in the IPA, it may nevertheless be criminalised by the WTA if wireless telegraphy apparatus is used without lawful authority with the intention of obtaining information about the sender, content or addressee of a message, or where information obtained in this way is disclosed.[16] The use of hidden recording devices for covert surveillance may be caught by these provisions.

UK General Data Protection Regulation

On the UK's departure from the EU, the government incorporated the GDPR into domestic legislation, creating the 'UK GDPR'. A series of amendments were then introduced to the UK GDPR by means of Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019/419. However, in reality, the data protection regime existing prior to 31 December 2020 remains the same. Pending a data protection adequacy decision by the European Commission (EC), the Trade and Co-operation Agreement (TCA) between the UK and EU stipulates that the UK data protection laws will not diverge from those of the EU for a specified period until April 2021, automatically extendable to June 2021 unless either party objects.

The UK GDPR applies to personal data processing by organisations operating within the UK, and to those operating outside the UK offering goods or services to individuals in the UK.[17] It does not apply to processing by 'competent authorities' (e.g., the police or Crown Prosecution Service) for law enforcement purposes, to intelligence service processing (e.g., the Security Service or Secret Intelligence Service), or to processing by individuals for purely domestic or household activities.[18]

Article 5 of the UK GDPR stipulates that personal data must be processed in accordance with seven principles:

- it must be processed lawfully, fairly and transparently (lawfulness, fairness and transparency);
- it must not be processed in a manner incompatible with the specific, explicit and legitimate purposes for which it was originally collected (purpose limitation);

12 Section 253 of the IPA.
13 Section 253(1) of the IPA.
14 Section 254 of the IPA.
15 See Part 8, Chapters 1 and 2 of the IPA.
16 Section 48 of the WTA.
17 Article 3(2)(a) of the UK GDPR.
18 Article 2(2) of the UK GDPR.

- it must be limited to what is necessary in relation to the purpose for which it was collected (data minimisation);
- it must be accurate and kept up to date (accuracy);
- it must not be kept for longer than is necessary (storage limitation);
- it must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality) and
- data controllers must be able to demonstrate compliance with the principles relating to personal data processing (accountability).

Breaches of these principles can lead to the imposition of substantial administrative fines imposed by the Information Commissioner's Office (ICO). The ICO may also prosecute offenders in the criminal courts for offences under the DPA (see below) and CMA. Those suffering damage (including distress) from breaches of the data protection legislation may seek compensation from the controller or processor concerned.

Amplifying the lawfulness, fairness and transparency principle, Article 6 of the UK GDPR provides six bases for the lawful processing of personal data including consent, compliance with a legal obligation, legitimate interest, and the public interest.

The UK GDPR also distinguishes between personal data and 'special category' personal data, the latter including data identifying a person's sexual orientation, political opinions, ethnic origin, health data or constituting biometric data.[19] Under Article 9, the processing of such data is unlawful unless one of the exceptions in Article 9(2) applies, the most obvious being the presence of explicit consent (the word explicit implying a higher degree of consent than under Article 6).

The UK GDPR provides a comprehensive legal mechanism for modern data handling. It stipulates penalties for breaches but allows for the restriction of the scope of rights and obligations to safeguard matters such as public security, the prevention and detection of criminal offences, and other important objectives of general public interest.

Data Protection Act 2018

The DPA, as amended by Schedule 2 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019/419, regulates the processing of data by 'competent authorities' (e.g., the police, Serious Fraud Office, Financial Conduct Authority (FCA) and National Crime Agency (NCA) and the intelligence services). In addition, it complements, amplifies and provides exemptions from, the provisions of the UK GDPR. The DPA also contains provisions concerning the ICO, including its enforcement powers.

Subject to certain statutory defences, the DPA criminalises certain behaviour in relation to personal data, including knowingly or recklessly obtaining or disclosing it without the consent of the controller (blagging). It also makes it an offence to retain personal data without the consent of the controller from whom it was obtained; to offer or sell 'blagged'

19 Article 9 of the UK GDPR.

personal data; to 're-identify' personal data that has been de-identified (i.e., processed in such a manner that, without more, it can no longer be attributed to a particular data subject) without the controller's consent; or to process such re-identified data.[20]

Network and Information Systems Regulations 2018

The Network and Information Systems Regulations (NISR) apply to operators of essential services (OES)[21] (e.g., water, transport and energy) and relevant digital service providers (RDSPs)[22] (e.g., online search engines available to the public, online markets and cloud computing services). NISR requires appropriate and proportionate technical and organisational measures to manage the risk of disruption. Incidents significantly impacting essential service continuity must be notified to the applicable competent authority.[23] Where incidents are suspected of having a cybersecurity element, operators are also strongly encouraged to contact the National Cyber Security Centre (NCSC).

NISR was reviewed in May 2020 and the government is considering amendments to its provisions about costs recovery and appeals against Competent Authority decisions.

Police Act 1997 and Intelligence Services Act 1994

Actions that would otherwise be considered breaches of law are made lawful when conducted by state agencies principally in the interests of national security, and for the prevention and detection of serious crime, in accordance with the various authorisation regimes established under IPA, the PA and the ISA.

Part III of the PA provides for authorities to interfere with property where it is necessary and proportionate. Authorisation may be issued by an authorising officer or with prior approval of a Judicial Commissioner where the property affected is someone's home, office premises or where the action may result in acquiring knowledge of confidential, journalistic or legal professional privilege (LPP) material.

The ISA provides a mechanism, on an application by the Security Service, Intelligence Service or GCHQ, for the Secretary of State to authorise interference with property or wireless telegraphy (subject to the requirements of necessity and proportionality).[24]

Relevant law enforcement agencies and other bodies

The primary law enforcement agencies with responsibility for regulating and enforcing the UK's cyber laws are the ICO[25] and the NCA[26]. The NCSC[27] performs a preventative and coordination role in the event that serious incidents occur, deploying expert technical skills to mitigate the impact. Where national security is at risk, the UK's security and intelligence agencies will also be involved.

---

20 See sections 170 and 171 of the DPA.

21 See Part 3 of the NISR.

22 See Part 4 of the NISR.

23 See, for example, Regulation 11 of the NISR.

24 See sections 5–7 of the ISA.

25 https://ico.org.uk.

26 https://nationalcrimeagency.gov.uk.

27 www.ncsc.gov.uk.

The ICO enforces the DPA and the UK GDPR in the civil arena, and the DPA in the criminal sphere. It is also involved in the regulation of relevant digital service providers under the NISR (see above), regulates organisations engaging in electronic marketing or using cookies,[28] and is the supervisory body for the regulations relating to electronic signatures and online transactions.[29]

The law enforcement body with primary responsibility for investigating and prosecuting cyberattacks is the NCA. The NCA's National Cyber Crime Unit (NCCU) works in conjunction with the UK's Regional Organised Crime Units, the Metropolitan Police Cyber Crime Unit and other national and international strategic partners to tackle serious and organised crime including cyber-attacks. The NCCU tackles serious cybercrime incidents both nationally and internationally and offers technical assistance within the NCA itself and to other law enforcement agencies, including through technical interception of communications. It also gathers and coordinates intelligence of serious and organised crime using traditional policing methods such as covert human intelligence sources, undercover officers and technical interception of communications.

Voluntary disclosure to the NCA of information relevant to its functions is encouraged using the information sharing gateway created by the Crime and Courts Act 2013, which absolves informants using it from actions for breach of confidence in the UK and disapplies other restrictions on disclosure.[30] As with other offences, criminal cases prosecuted by the NCA must satisfy the Full Code Test in The Code for Crown Prosecutors,[31] meaning there must be a reasonable prospect of a conviction and also that any prosecution must be in the public interest.

The NCSC protects critical services from cyberattacks, managing major incidents and improving underlying security through advice and guidance on threat reduction and incident management to all sectors, from individuals to large organisations and the public sector.[32] The NCSC has attracted widespread admiration though some observers have expressed concern that its resources may become overstretched as demand grows for its expertise and assistance to deal with swiftly evolving cyber threats.[33] The coronavirus pandemic has added to the NCSC's burden, as it has been instrumental in ensuring the safe and effective functioning of NHS Trusts during this period.[34]

In February 2020, the UK government announced an Integrated Review of Security, Defence, Development and Foreign Policy,[35] which will help to shape the UK's national approach on cyber security beyond 2021. It is expected that the NCSC will play a major role in bolstering the UK's cyber security defences going forward.

In addition to the ICO, the NCA and the NCSC, other bodies have assumed secondary regulatory oversight roles for cybersecurity. For example, under Principle 11 of the Financial

28 Through the Privacy and Electronic Communications (EC Directive) Regulations 2003/2426, now retained EU law under the European Union (Withdrawal) Act 2018.

29 Electronic Identification and Trust Services for Electronic Transactions Regulations 2016, also retained EU law.

30 Crime and Courts Act 2013, Section 7.

31 www.cps.gov.uk/publication/code-crown-prosecutors.

32 www.ncsc.gov.uk/section/about-ncsc/what-we-do.

33 https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/170808.htm.

34 See NCSC annual report 2020: www.ncsc.gov.uk/annual-review/2020/index.html.

35 www.gov.uk/government/collections/integrated-review-ministry-of-defence.

Conduct Authority (FCA) Handbook, regulated firms must notify the FCA of 'material cyber incidents' (i.e., those resulting in significant data loss affecting a large number of customers, or result in unauthorised access to, or malicious software on, information and communications systems).[36] The FCA offers tools by which firms conducting regulated activities may assess their cyber resilience. Where a firm is registered with the Prudential Regulation Authority (PRA), it should also report cyber incidents to the PRA.[37]

ICO enforcement regime

The ICO is the independent supervisory authority responsible for monitoring the application of the UK GDPR. The ICO's tasks are enumerated in the UK GDPR,[38] and they include monitoring and enforcement, promoting awareness of the obligations of controllers and processors, and providing mutual assistance to overseas supervisory authorities.

ICO investigations may start in a variety of ways, including a complaint by a data subject, information received from other regulators,[39] or of its own volition where the ICO has a concern about a particular sector. The ICO may also commence investigations as a result of whistle-blowing information, and the Information Commissioner is a 'prescribed person' under the Public Interest Disclosure Act 1998, meaning that qualifying disclosures to the ICO (e.g., a worker's reasonable belief that a crime has been committed or that a person is failing to comply with a legal obligation) should not give rise to any detriment to the informant. Between 1 April 2019 and 31 March 2020, 427 whistle-blowing disclosures were made to the ICO, and the regulator took further action in relation to 16 per cent of these.[40]

The ICO's specific enforcement powers are detailed in Parts 5 and 6 of the DPA, and include the right to seek a warrant of entry and inspection where controllers or processors of personal data are suspected of failing to comply with certain UK GDPR provisions, or where a criminal offence under the DPA is suspected.[41] However, unless a judge is satisfied that the matter is urgent or that advance warning of the search would defeat the object of entry to the target premises, the ICO must give seven days' notice in writing to the occupier as one of several preconditions for the issue of a search warrant.[42] Nevertheless, prudent controllers and processors will have a 'dawn raid' plan in place for 'no-notice search warrants'. Such plans would include ensuring reception staff know who to contact and having an internal and external team in place to deal with incidents, including the identification of legally privileged material that is exempt from inspection and seizure.[43]

It is a criminal offence to intentionally obstruct the ICO in the execution of a search warrant, to fail to provide reasonable assistance in the execution of the search warrant without reasonable excuse, or to give a deliberately or recklessly false explanation of any document or other material found on the premises.[44] During the execution of a search warrant,

36 www.handbook.fca.org.uk/handbook/PRIN/2/1.html?date=2016-03-07.

37 https://www.fca.org.uk/firms/cyber-resilience .

38 UK GDPR Articles 57 & 58 respectively.

39 https://ico.org.uk/about-the-ico/our-information/working-with-other-bodies/.

40 https://ico.org.uk/about-the-ico/our-information/whistleblowing-disclosures/.

41 Section 154 and Schedule15 of the DPA.

42 Schedule 15, para 4 of the DPA.

43 Schedule 15, para 11 of the DPA.

44 Schedule 15, para 15 of the DPA.

occupiers should make careful records (and where possible take copies) of all information and systems accessed by the ICO. The ICO may exercise reasonable force when executing a search warrant.[45]

The ICO has published a Regulatory Action Policy (RAP),[46] listing its regulatory objectives, adumbrating on the nature of its powers, and setting out how the ICO will select appropriate regulatory activity for breaches of information rights. The RAP indicates that, as a general principle, more serious breaches (e.g., where there is a high impact, the breach was intentional, or where there are recurring breaches) may expect stronger regulatory action. In 2020, the ICO issued draft statutory guidance detailing how the regulator will take regulatory action against organisations and individuals, emphasising the ICO's risk-based approach, and explaining the method by which it calculates penalties.[47]

Article 83 of the UK GDPR sets out two categories of UK GDPR infringement, each with different penalties. The first category carries a maximum penalty of up to 2 per cent of a business' global annual turnover or up to £8.7 million, whichever is the greater. Included in this first category is a failure to take adequate security measures to protect personal data. Also included in this category are failures to comply with record-keeping obligations; failures to designate a data protection officer when required to do so; and failures to cooperate with the ICO. The second category of offence carries a maximum penalty of up to 4 per cent of a business' global annual turnover or £17.5 million, whichever is greater. Within this category are individual offences related to the processing principles, the rights of data subjects and obstruction of the ICO.[48] The lists of infringements in both categories are not exhaustive, and may be expanded in the future.

Before issuing a penalty notice, the ICO must serve a notice of intent, setting out the circumstances of the breach, the ICO's investigation findings, and the proposed level of penalty. The recipient then has 21 days in which to make representations about the imposition of a penalty and its level, before the ICO reaches its final decision.[49] In the first instance, appeals lie to the First Tier Tribunal (Information Rights).[50]

The RAP suggests that the heaviest penalties will be imposed on organisations that repeatedly and wilfully transgress their obligations, and where formal regulatory action would serve as a deterrent to others. When deciding on the level of the penalty imposed, the ICO will take into account aggravating factors (e.g., whether an organisation has made any financial gain as a result of the failure to report), and mitigating factors such as economic impact of the penalty and ability to pay. Deliberate failure, the involvement of vulnerable victims or a poor regulatory history, are likely to increase the size of the penalty imposed.

In addition to its civil enforcement powers, the ICO may prosecute criminal offences in the DPA.[51] Those convicted of such offences may only be fined.[52] However, the ICO has

45 Schedule 15, para 7 of the DPA.

46 https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.

47 https://ico.org.uk/media/about-the-ico/consultations/2618333/ico-draft-statutory-guidance.pdf .

48 Article 83(6) of the UK GDPR.

49 See page 25 of the ICO's Regulatory Action Policy.

50 Section 162 of the DPA.

51 For example, sections 170–173 of the DPA.

52 Section 196 of the DPA.

found creative ways of overcoming this limitation, securing custodial sentences through prosecuting instead for CMA offences.[53]

ICO enforcement activity

Future data regulatory divergence between the UK and EU may render comparisons of regulatory activity between the ICO and EU Member State's respective data supervisory authorities difficult. For the time being, however, the UK and EU regulatory regimes are essentially equivalent, and meaningful comparisons remain possible. Judged by the level of GDPR penalties imposed, the ICO is one of the toughest regulators: only Italy, Germany and France imposed fines of larger overall value in the period May 2018 to January 2021, and the UK imposed the fourth and fifth largest GDPR penalties of all EU data supervisory authorities in the same period.[54]

Resourcing is a constant issue for data regulators when taking enforcement activity against some of the world's wealthiest companies; underfunding of data supervisory authorities was a universal issue mentioned by the EC in a report published in 2020 to mark the two-year anniversary of the GDPR's implementation.[55] Even the comparatively well-funded ICO was nevertheless believed to employ only 22 specialist technical investigators, and its resources were less stretched during the pandemic as regulatory activity was pared back. As activity levels normalise, the ICO anticipates that its spend will increase in key areas, heralding increased regulatory work and greater pressure on its resources.

Non-state authority investigations

Although relatively well-resourced, UK law enforcement's cyber capability inevitably faces practical limits on its ability to tackle increased levels of cybercrime. Just as other areas of crime have seen increasing interest in private prosecutions, victims of cybercrime may in future wish to take active steps to conduct their own cyber investigations, including 'active defence' (colloquially known as 'hacking back'). However, in the UK such steps are significantly hindered by the manner in which the law is cast. This is particularly so given how the broadly constituted 'unauthorised access' element of the CMA works to criminalise actions even if taken to protect the rights and properties of a 'victim', [56] the way in which the UK's data protection legislation safeguards personal data, and the requirement that prosecutions for DPA offences are brought only by the ICO or with the Director of Public Prosecutions' consent.[57] In such ways, the law provides a real barrier to an investigation by non-public entities that feel they have been wronged and suffered damage. In consequence, such entities are effectively limited to working with computers and data they either control, or to which voluntary access is given. However, voluntary access may not be forthcoming given the

53 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/six-month-prison-sentence-for-motor-industry-employee-in-first-ico-computer-misuse-act-prosecution/ & https://ico.org.uk/action-weve-taken/enforcement/kim-doyle-and-william-shaw/.

54 British Airways and Marriott International Inc.

55 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0264&from=EN.

56 See sections 1 & 2 of the CMA.

57 Section 197 of the DPA.

potential liabilities that may result, not only for those giving access, but also for intermediaries facilitating it.

Without being granted voluntary access to third-party data, those undertaking private investigations will need to seek the assistance of the courts in the form of *Norwich Pharmacal* orders, obliging innocent third parties caught up in wrongdoing to disclose the identity of perpetrators of cybercrime. However, seeking such orders may still be costly and time-consuming. Alternatively, private investigators may seek the assistance of the relevant authorities, likely to be the NCA (subject always to the NCA having a necessary criminal justice justification for acting).

Privileged investigations in the United Kingdom

Regardless of whether an investigation is internal or being undertaken by external agencies, legal professional privilege is likely to be a significant consideration, and this applies equally to cyber investigations. Indeed, in some respects it is difficult to imagine an investigation that does not involve some element of electronic data and information technology and computer networks.

Whatever the genesis and form of a cyber investigation, it will be important to bear in mind the definitions of privilege and the complex rules that are features of it.

In very broad terms, legal advice privilege attaches to communications between a client and a lawyer in connection with the giving or receiving of legal advice. Litigation privilege attaches to documents created for the dominant purpose of conducting existing or reasonably contemplated adversarial litigation (here, privilege may extend to third parties as well as clients and lawyers). Crucial to establishing and maintaining either form of privilege, particularly in the face of investigations by regulators and law enforcement, are the existence of client–lawyer (including in-house lawyer) relationships and confidentiality of documentation. In most circumstances, privilege does not attach to pre-existing documents or non-privileged email attachments merely by sending such material to lawyers.

Those involved in an investigation should have the following points in mind from the earliest stages:

- External legal counsel should be engaged promptly to ensure the requisite creation of a client–lawyer relationship. While privilege attaches to communications between a client and in-house counsel, the role of such lawyers is not always exclusively the provision of legal advice. To avoid arguments about the dominant purpose of in-house counsel's communications, it may be prudent to engage external lawyers from the outset.
- The nature of the advice sought should be referred to in outline in the letter of engagement if privilege over that document is to be maintained.
- The identity of the 'client' should be carefully established from the outset, preferably in the letter of engagement. Legal advice privilege attaches only to communications between lawyers and a client (or a client's agent in certain circumstances), that is, those individuals tasked with seeking and receiving legal advice on behalf of an entity.
- Since confidentiality is a prerequisite for the existence of privilege, care should be taken to ensure privileged material is circulated only on a need-to-know basis. Before sharing detailed information with third parties such as insurers, non-disclosure agreements should be negotiated.

- Where privileged material is referenced at internal meetings, it may be prudent to record privileged discussions in a separate document rather than in general minutes. Similarly, warnings should be given about making manuscript notes of privileged advice that may in themselves not be privileged.
- All legally privileged material created during the course of an investigation should be marked appropriately, for example by including the words 'Confidential – Subject to Legal Professional Privilege'. While characterising communications in this way is not determinative of privilege, it should raise the issue in the mind of any external regulators and law enforcement, will assist subsequent identification, and may ensure caution is exercised when disseminating communications.
- Since litigation privilege attaches only where adversarial proceedings are in reasonable contemplation at the time a particular communication is made, careful consideration must be given to whether the facts give rise to the necessary circumstances.
- The use of third parties (e.g., an external IT forensic team) should be carefully considered and care must be taken to ensure their work is protected by privilege – generally by ensuring instruction through external counsel appointed to advise on or handle the investigation.

While regulators and law enforcement are not permitted to seize privileged communications, when they exercise their investigatory powers, there are inevitably circumstances in which it is not possible to separate privileged from non-privileged material onsite. In such circumstances, provision is made allowing for the uplifting and subsequent sift of such 'mixed material'.[58] Where electronic data is seized in this way, electronic search terms are often sought to identify privileged (and relevant) material. Those advising individuals and companies whose material has been seized will wish to ensure that any risk to their clients' privilege is minimised during this process.[59]

Cyber investigations – cross-border data sharing

In the context of cross-border investigations, there is now a discernible trend towards greater international sharing of information and evidence, no more so than in cyber investigations.

Recognising that increased information exchange and international cooperation is key to tackling cross-border crime, the Crime (Overseas Production Orders) Act 2019 (COPOA) has been enacted to facilitate the expedited sharing of electronic data between law enforcement bodies in the UK and countries with which the UK has a 'designated international cooperation arrangement'.[60] In reality, the COPOA was drafted specifically to provide for electronic data sharing with the US and to overcome the lengthy delays experienced with Mutual Legal Assistance requests.[61] However, there is no statutory reason that similar treaties may not be agreed with other nations. The EC has itself proposed the introduction of overseas production and preservation orders that would bring about similar cross-border

58 Criminal Justice and Police Act 2001, Part 2.

59 *R (McKenzie) v. Director of the Serious Fraud Office* [2016] EWHC 102 (Admin).

60 Crime (Overseas Production Orders) Act 2019, Section 4(2).

61 See the House of Lords Briefing on the Crime (Overseas Production Orders) Bill: file://vbclfile/Home$/jhayes/Downloads/LLN-2018-0076%20(3).pdf.

electronic data exchange throughout the EU. Before the UK departed the EU, the UK government had expressed reservations about participating in the pan-EU proposal, citing a reluctance to share data with more authoritarian EU Member States, along with a fear that participating might undermine the operation of the bilateral US–UK electronic data sharing agreement, which was seen as more significant for UK law enforcement.

Under the COPOA, appropriate officers of law enforcement agencies including the SFO, FCA and HMRC may apply to Crown Courts in England Wales for an order directly requiring overseas service providers to produce or grant access to electronic data for the purposes of investigating and prosecuting indictable or terrorist offences.[62] Respondents must be given notice of applications unless the court directs otherwise, allowing for representations on the scope of the application, and practicality of compliance before any order is made. Recipients of an order would be expected to produce the data within a specified time frame on pain of contempt proceedings.[63] Further procedural details may be found in the Criminal Procedure Rules.[64] The UK–US bilateral agreement and the COPOA are expected to begin operating during 2021.

Cyber regulatory trends

Governments around the world have been re-examining existing models of online regulation for some time, and the UK has been at the forefront of this trend, particularly in the fields of online harms.

Following a 2019 online harms consultation, the government has published its full response.[65] Aimed at both illegal online harms such as terrorist content, child sexual exploitation and abuse material, and legal but harmful material such as cyberbullying and promotion of self-harm, the proposals will introduce a duty of care on service providers to take action to prevent user-generated content or activity on their services from causing significant physical or psychological harm to individuals. All service providers will be obliged to take action against illegal content and activity. Where children may use a service providers' products, those providers must also protect children against legal but harmful content and activity. High-risk 'Category 1' providers[66] will have additional obligations in respect of legal but harmful content accessed by adults. The government has declined to include investment fraud and other financial scams in the scope of its online harms proposals, though the FCA, trade bodies and consumer groups have called for their inclusion because of their prevalence. The online harms regime will be enforced by the communications regulator Ofcom, which will have the power to impose administrative penalties of £10 million or 10 per cent of the parent company's annual global turnover (whichever is the higher). Draft legislation is expected during 2021.

62 See Sections 1–15 of the COPOA.

63 Criminal Procedure Rule 47.68.

64 Criminal Procedure Rules 47.66–47.71.

65 www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response.

66 To be determined by size and the functionalities offered.

Implications of Brexit for UK data regulation and cyber investigations

In February 2021, the EC published draft adequacy decisions in the UK's favour under the GDPR and Law Enforcement Directive,[67] which are likely to be adopted later in the year. As a 'bridging' measure to preserve the £127 billion of personal data-enabled trade between Europe and the UK,[68] the TCA agreed between the UK and EU provided that the UK shall not be treated as a 'third country' for cross-border data transfers for four months from 1 January 2021, automatically extended to six months unless either side objects. This 'holding position' was conditional on the UK not changing its data protection laws and the ICO not approving new data transfer mechanisms or codes of conduct without prior EU consent during the four to six month period.[69] UK data regulation is therefore unlikely to change in the short term.

Looking to the future, though, the government's National Data Strategy,[70] with its implicit aim of alleviating the burden of the current data regime on SMEs, its overt mission to champion international data flows, and a new Information Commissioner in office from October 2021 whose job specification emphasises the economic potential of data and avoiding unnecessary barriers to its use, suggest the UK's data protection regime will change once the EC's adequacy deliberations are concluded. The significance of such changes will only emerge over time, but divergence will mean that an adequacy decision in the UK's favour may be vulnerable not only to the risk of challenge in the Court of Justice of the European Union by data activists, but also to the possibility of withdrawal by the EC itself.[71] The economic risks posed by data inadequacy[72] may, however, moderate the UK's appetite for deviating from EU data regulation standards.

During the early stages of the Brexit talks, ministers were hopeful of continuing close cooperation between the UK and EU over cybersecurity, and the UK's expertise in this area was perceived as a negotiating advantage. However, the TCN deals only briefly with cybersecurity with the UK and EU agreeing to 'endeavour to establish a regular dialogue' in relation to such matters.[73] The UK may – by invitation – participate in certain activities with the EU's Cybersecurity Agency ENISA, CERT EU[74] and the EU CSIRT network.[75] In practice, given the international nature of cyber threats and the UK's capability in these areas, close but low-key UK-EU cooperation will likely continue.

At a more day-to-day law enforcement level, the UK will retain access to EU passenger name records, and the Prüm database of biometric data, which may in future be expanded to include facial recognition data. The UK will no longer be a member of the EU's law enforcement agency, Europol, but it may second staff there to enhance cross-border cooperation, and UK law enforcement will have access to Europol's secure messaging service. Adequacy

67 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L0680.

68 www.ucl.ac.uk/european-institute/sites/european-institute/files/ucl_nef_data-inadequacy.pdf..

69 TCA, Part 7 Final Provisions, Article FINPROV 10A Interim provision for transmission of personal data to the United Kingdom.

70 www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy.

71 By means of EU GDPR Art. 45(5).

72 See footnote 67.

73 TCN Part 4 – Thematic Co-operation, Title 2 Cyber security.

74 The Computer Emergency Response Team which responds to information security incidents and cyber threats.

75 Dealing with network and information systems.

decisions in the UK's favour should cement continued cooperation, which is surely in the interests of both the UK and EU. Significantly, however, the UK will not have access to the Schengen Information System, SIS II, Europe's largest public security information database offering 'real-time' alerts on wanted and missing persons or objects across the EU. UK police checked SIS II 600 million times in 2019, and its loss will hamper the speed and accuracy of UK law enforcement activity, as UK law enforcement is now left reliant on INTERPOL's Red Notice and diffusion databases to which not all EU Member States routinely upload.

Julian Hayes
BCL Solicitors LLP

Julian Hayes advises companies and individuals in the rapidly developing field of data protection, especially in the context of data breaches and law enforcement investigations, where necessary litigating to ensure that the actions of state authorities are properly constrained. A partner at BCL for four years, he has vast experience of all types of criminal inquiries, including the unlawful obtaining of data and computer misuse offences. He is well-known and highly regarded commentator on cybersecurity and privacy issues. He advises telecommunications operators on their obligations under UK investigatory powers legislation and provides practical guidance on how to handle demands placed upon them, including in establishing systems that work to ensure legal compliance and protection for the operator. He has advised in relation to US–UK Bilateral Data Sharing Agreement and forthcoming UK online harms legislation.

Michael Drury
BCL Solicitors LLP

Michael Drury's expertise in data collection and surveillance matters by state entities is unparalleled in the United Kingdom. As a former director of legal affairs at GCHQ, the largest of the UK's security and intelligence agencies, for 14 years; founder member of the Serious Fraud Office; and for the last 10 years a partner in BCL providing advice on national security and criminal investigations to both corporate and individual clients, his breadth of experience both in terms of developing legislation (particularly the Regulatory Investigatory Powers Act as the forerunner to the current Investigatory Powers Act 2016) and practical casework gives him unique insights into how the law has developed and the practical consequences that follow. He has already provided advice on the US–UK Bilateral Data Sharing Agreement due to commence this autumn and brings his breadth of knowledge to bear on what is a new departure in a field that is inherently controversial.

BCL Solicitors LLP
51 Lincoln's Inn Fields
Holborn
London WC2A 3LZ
United Kingdom
Tel: 020 7430 2277
jhayes@bcl.com
mdrury@bcl.com
www.bcl.com