Explanatory Framework for Adequacy Discussions

Section H: National Security Data Protection and Investigatory Powers Framework

Overview

This section systematically goes through the UK legislation governing the operation of the UK's national security and investigatory powers framework.

PART I: OVERARCHING NARRATIVE

Overview

This section will set out the key aspects of legislation and safeguards relating to the processing of data for national security purposes and the use of investigatory powers. It will explore in detail the UK legislation that provides for unprecedented independent oversight of the operation of the UK's national security and investigatory powers framework.

The processing of personal data by the UK's Intelligence Community (UKIC)[1] is governed by Part 4 of the Data Protection Act 2018 (DPA 2018), while a comprehensive legislative framework applies to their use of investigatory powers. The UK government has placed data protection and privacy at the heart of the DPA 2018 and the Investigatory Powers Act 2016 (IPA).

This approach was most recently noted by the UN Special Rapporteur for the Right to Privacy, Joseph Cannataci who, after conducting an extensive review of the UK's investigatory powers framework in 2018, assessed the UK as having:

> *"...equipped itself with a legal framework and significant resources designed to protect privacy without compromising security. Given its history in the protection of civil liberties and the significant recent improvement in its privacy laws and mechanisms, the UK can now justifiably reclaim its leadership role in Europe as well as globally."*[2]

The Special Rapporteur further noted:

> *"I am satisfied that the UK systematically employs multiple safeguards which go to great lengths to ensure that unauthorized surveillance does not take place, and that when authorization is sought it is granted only after the necessity and proportionality of the surveillance measure are justified on a case-by-case basis."*

The UNSR also stated at the recent International Intelligence and Oversight Forum (IIOF) 2019, that the UK edition of the IIOF demonstrated:

> *"the significant reinforcement of oversight mechanisms in the UK since 2016 and thus several best practices, including some pioneered by the UK, could be explored by the participants."*[3]

[1] The Security Service (MI5), Secret Intelligence Service (SIS) and Government Communications Headquarters (GCHQ), are hereafter referred to as the UK Intelligence Community (UKIC).
[2] https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23297&LangID=E
[3] IIOF, 2019

Data processing for national security purposes

Introduction

Investigatory powers are available to a range of specified public authorities in the UK and can be used for a range of detailed purposes, including for national security related investigations/operations. The data obtained by the authorities using these powers is processed under a range of legislation, providing multiple layers of protection and safeguards to data subjects. A key basis of this protection is the **DPA 2018**, which replaced the Data Protection Act 1998.

In addition to the safeguards and limitations provided for by the DPA 2018, the **IPA applies further protections and restrictions on the acquisition, retention, handling, and use of communications and communications data** acquired by public authorities, as well as the Security Services Act 1989 (SSA) and Intelligence Services Act 1994 (ISA).

These additional protections reflect the particular sensitivity and privacy considerations which appropriately apply to the state's access to communications. The safeguards and limitations in these pieces of legislation are set out below and in further detail in the other parts of this document.[4]

Alongside the DPA 2018, the Human Rights Act (HRA) 1998 underpins and is a key component of the tiered protection provided to data subjects in the UK. Section B of this pack (Wider Context) contains more detail on the HRA and the European Convention on Human Rights (ECHR). The HRA places a duty on public authorities to act compatibly with human rights and enables individuals to enforce those rights directly in courts in the UK. Article 8 of the ECHR provides that any interference with privacy must be in accordance with the law, in the interests of one of the aims set out in Article 8(2) and proportionate in light of that aim.

The safeguards provided for in the IPA reflect the UK's international reputation for protecting human rights, including the right to respect for a private and family life in Article 8 of the ECHR. Article 8 also requires that the interference must be "foreseeable" – that is, have a clear, accessible basis in law – and that the law must contain appropriate safeguards (authorisation checks, as well as scrutiny, oversight and redress mechanisms) to prevent abuse.

All these statutory protections are supported internally by rigorous physical, technical, and procedural requirements. These include vetting of personnel, additional handling

[4] This section provides information about the UK's investigatory powers framework as a whole, notwithstanding that not all powers may be relevant to the essential equivalence test because, for example, they may not be used in the context of personal data transferred from the EU.

restrictions based on the classification of data, firewalling of internal IT, and access restrictions based on the established principle of 'need to know'. These controls provide for strong protections for personal data and ensure in particular that it is held securely.

Summary of the DPA 2018

The processing of personal data for national security purposes can fall within any of the three data protection regimes under the DPA 2018.

- The UK General Data Protection Regulation ("UK GDPR") applies to data processed for national security purposes where the controller is neither one of the UKIC agencies (or processing on their behalf), nor a competent authority (e.g. a police force) which is processing for a law enforcement purpose.

- Part 3 of the DPA 2018 applies to data processed by a competent authority for law enforcement purposes.

- Part 4 of the DPA applies to all processing of personal data by or on behalf of UKIC. The data protection standards in Part 4 of the DPA reflect those set out in the modernised Council of Europe Convention 108 (C108+). These are detailed in Part II of this section.

Part 4 of the DPA is not UKIC's only obligation when processing personal data. **To a greater extent than any other controller**, UKIC is subject to additional safeguards, oversight, and scrutiny covering how they process data (which includes collection, analysis and retention).

More detail about the DPA 2018 is contained in Part II of this section.

Summary of the IPA

The IPA[5] introduced unprecedented transparency and world leading privacy, redress, and oversight arrangements which strengthen previous safeguards, such as those set out in the Regulation of Investigatory Powers Act 2000 (RIPA), applying to the use of investigatory powers.

The IPA **makes clear the circumstances** in which various investigatory powers may be used and **the strict safeguards** that apply, ensuring that any interference with privacy is strictly necessary, proportionate, authorised, and accountable.

The IPA requires that the use of investigatory powers must **always** be justified on the grounds of both **necessity and proportionality**: it must be necessary for the purpose

[5] The development of the IPA was also underlined by Lord Anderson's June 2015 report "*A Question of Trust"* [see supplementary material]. This report considered the balance between security and human rights in a post 9/11 and 7/7 environment.

specified; and the action authorised must be proportionate to the outcome sought to be achieved. This means that:

- if an interference with privacy is not necessary, it cannot be lawful; or
- if some level of interference is necessary, but the actual interference being proposed would be disproportionate to that end, then it would also be unlawful.

The IPA sets out general duties regarding privacy[6] to make clear that the protection of privacy is at the heart of this legislation. Public authorities must have regard to:

- whether the same effect could reasonably be achieved by less intrusive means;
- whether a higher level of protection is required because targeted information is particularly sensitive (e.g. legally privileged material, journalistic material including that identifying a source, communications of members of Parliament);
- the public interest in the integrity and security of telecommunications systems.

Lord Anderson QC, the former Independent Reviewer of Terrorism Legislation – supported by an expert team of his own choosing – concluded in a report in 2015 which set out the operational case for these powers and the need to update such legislation that:

> *"Whether a broader or narrower definition is preferred, it should be plain that the collection and retention of data in bulk does not equate to so-called "mass surveillance". Any legal system worth the name will incorporate limitations and safeguards designed precisely to ensure that access to stores of sensitive data is not given on an indiscriminate or unjustified basis. Such limitations and safeguards certainly exist in the [Investigatory Powers] Bill."*[7]

The IPA's legislative framework is supported by statutory codes of practice[8] on each of the key investigatory powers, providing a transparent and comprehensive explanation of how powers are to be used by public authorities. The public authorities using investigatory powers are required to have regard to the codes of practice when carrying out conduct under the IPA.

Failure to comply with the codes of practice does not, of itself, make a person liable to criminal or civil proceedings. However, the codes are admissible as evidence in criminal and civil proceedings. Any court or tribunal considering such proceedings, the Investigatory Powers Tribunal (IPT), Investigatory Powers Commissioner (IPC) responsible for overseeing

[6] Section 2 of the IPA
[7] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF, p. 4.
[8] Schedule 7 to the IPA

the powers and functions conferred by the Act, or the Information Commissioner, may take the provisions of the codes and failure to comply with the codes into account.

The IPA also introduced a **double lock** mechanism**,** whereby a decision by the Secretary of State, (or Scottish Minister and in certain circumstances, a law enforcement chief) is required to authorise specific use of the most intrusive powers, and is also subject to mandatory review and approval by an independent Judicial Commissioner before it can have legal effect**.**

Moreover, individuals who believe themselves to have been subject to unlawful surveillance have the right to redress by bringing a case before the IPT.

Above all, the safeguards in the IPA continue to reflect the UK's international reputation for protecting human rights. This unprecedented transparency sets a new international benchmark for how the law can protect both privacy and security whilst continuing to respond dynamically to an evolving threat picture.

Further detail on the IPA's safeguards is contained in Part III of this document.

Summary of the SSA

The statutory basis under which MI5 operates is set out in the SSA. The SSA sets out MI5's functions: protecting national security; safeguarding the economic well-being of the UK against outside threats; and supporting activities of the police forces and other law enforcement agencies in the prevention and detection of serious crime.

The SSA places MI5 under the authority of the Home Secretary, who is accountable to Parliament for the Service's work. It also stipulates that a Director General must be appointed to ensure *"there are arrangements for securing that no information is obtained by the Service except so far as necessary for the proper discharge of its functions or disclosed by it except so far as necessary for that purpose or for the purpose of the prevention or detection of serious crime."*[9] The Director General is accountable to the Home Secretary.

Alongside this executive and parliamentary oversight is an independent oversight mechanism provided for by the independent IPC. The current IPC is Sir Brian Leveson (appointed October 2019): a senior judicial figure who was formerly the President of the Queen's Bench Division of the High Court and Head of Criminal Justice.

[9] Section 2(a) Security Services Act 1989

Summary of the ISA

The ISA provides a statutory footing for the functioning of the SIS and GCHQ. It mandates SIS and GCHQ to carry out their functions only in the interests of national security, economic well-being and to support in the prevention or detection of serious crime.

The ISA places both agencies under the authority of the Foreign Secretary. It requires that the Foreign Secretary appoint a Chief of SIS and a Director of GCHQ who have the equivalent statutory responsibilities of the Director General of MI5.

These statutory provisions place considerable constraints on the potential scope of agency activity and bring them under clear ministerial oversight. Oversight of investigatory powers activity is provided by the independent IPC, and redress by IPT, alongside parliamentary and judicial oversight.

Oversight and Redress

In addition to the extensive legislative framework, there is ministerial oversight and accountability; parliamentary oversight from the Intelligence and Security Committee (ISC) of Parliament; and independent oversight from both the Information Commissioner (powers and functions provided for in the DPA), and IPC, a role established under the IPA.

The Investigatory Powers Tribunal (IPT) is an independent judicial body that considers complaints by a person who believes that he or she has been the victim of unlawful interference by public authorities or has been the victim of a Human Rights violation. It also provides a right of appeal mechanism.

Further information can be found on oversight and redress mechanisms in Parts IV and V of this section respectively.

The rest of this document is structured into the following parts:

- Part II: Data Protection. This sets out the applicable data protection regimes for processing personal data for the purposes of national security.

- Part III: Powers. This outlines the investigatory powers under the IPA and RIPA, and their key safeguards. It covers:
    - Interception powers
    - Communications data powers, including for internet connection records
    - Equipment interference powers
    - Bulk powers
    - Bulk datasets
    - Powers under RIPA (obtaining access to protected electronic information)

- Part IV: Oversight. This explains the key oversight mechanisms, including the "double lock" for investigatory powers.

- Part V: Redress. This covers the redress mechanisms available to individuals who feel that they may have been the subject of unlawful surveillance.

PART II: DATA PROTECTION

Applicable protection regimes for processing personal data for the purposes of national security

There are three data protection regimes in the UK within the DPA 2018, all of which are capable of applying to the processing of personal data for national security purposes:

- The UK General Data Protection Regulation "UK GDPR"
- Law enforcement processing (Part 3 DPA 2018)
- Intelligence services processing (Part 4 DPA 2018)

The applicable regime will depend on both the **identity of the controller** and the **purpose** of the processing:

- The **UK GDPR** will apply
    - if data is processed for national security purposes and by a controller who is neither one of the intelligence services (or processing on their behalf) nor a "competent authority" (as defined in section 30 of the DPA 2018, e.g. a police force); or
    - if processing is by a "competent authority" but not conducted for a "law enforcement purpose" and is processed only for the purposes of national security.

  For example, a police force conducts security checks against an employee to ensure they can be trusted to access national security material. Despite being a competent authority, the processing in question is not for a "law enforcement purpose". Therefore Part 3 does not apply.
- **Part 3** of the DPA 2018 applies to data processed by a competent authority for law enforcement purposes.
- **Part 4** of the DPA 2018 applies to all processing by or on behalf of the intelligence services. The requirements of Part 4 are explained in a section below.

Data protection standards applicable to non-UKIC processing

As outlined in the applicability section above, processing for national security purposes may come under the UK GDPR, or Part 3 of the DPA 2018, depending on the identity of the controller and the purpose of processing.

Section H: National Security Data Protection and Investigatory Powers Framework

The provisions of the UK GDPR are set out in Section D of this pack ("Adequacy Referential") and thus are excluded from this section. The national security and defence exemption mentioned further below applies to specified provisions of the UK GDPR and DPA 2018. These are listed in section 26 of the DPA 2018.

The provisions of Part 3 are set out in Section F of this pack ("Law Enforcement") and thus are excluded from this document. The DPA 2018 also provides for national security "restrictions" for those operating under Part 3 of the Act, although this is only relevant to a more limited range of provisions in Part 3.

Data protection standards applicable to UKIC (Part 4 and other safeguards)

Scope

National security is outside the scope of EU law[10]. Consequently, the processing of personal data for national security purposes is not within scope of the EU's General Data Protection Regulation (EU GDPR) or the Law Enforcement Directive (LED). Recital 16 of the GDPR confirms that processing concerning national security activities is outside the scope of Union law and Recital 14 of the LED states that it does not apply to agencies or units dealing with national security issues.

As a result, the provisions of the EU GDPR and LED were not designed or indeed intended to be applicable to processing by the intelligence services. The DPA 2018 therefore **provides a specific data protection regime for the processing of personal data by or on behalf of UKIC** reflecting the standards provided for in the modernised Council of Europe Convention 108 (C108+).

C108+ reflects modern data protection standards and expectations, ensuring it keeps pace with developments. The Convention has a wider scope than equivalent EU data protection laws, as it applies to national security processing and national security agencies. As a result, the drafting of the Convention is designed to reflect this, ensuring that it can be applied appropriately to sensitive national security processing. The UK has taken the lead in giving effect to C108+ by adopting these standards in Part 4 of the DPA 2018.

Part 4 of the DPA 2018 provides a specific regime which applies to all processing of personal data by UKIC and persons processing personal data on behalf of UKIC. Due to the very nature of UKIC processing, handling sensitive data for national security purposes, UKIC necessarily have to adopt stringent standards when handling personal data (far higher than most controllers would need to).

[10] Article 4(2) TEU

This regime ensures that any processing of personal data by UKIC – whether or not it falls within restrictions imposed by other regulations such as the IPA is subject to appropriate and proportionate controls. It also ensures that it is calibrated in a way which recognises the critical role of the intelligence services in tackling the current and future threats to national security.

Part 4 of the DPA 2018 applies to processing by UKIC or processors under its control. Some of the key provisions in Part 4 of the DPA 2018 are provided in Chapter 2 and 3.

Principles for processing
Chapter 2 ("Principles") sets out the six data protection principles which apply to personal data processed under this Part of the DPA 2018:

- processing must be lawful, fair and transparent;
- the purposes of processing must be specified, explicit and legitimate;
- personal data must be adequate, relevant and not excessive;
- personal data must be accurate and kept up to date;
- personal data must be kept no longer than is necessary;
- personal data must be processed in a secure manner.

The first data protection principle requires the processing of personal data to be lawful, fair and transparent. There is no permitted exemption from the requirement that processing must be lawful.

This lawfulness requirement ensures that UKIC processing must comply with any relevant UK law and, in particular, the legislation governing the activities of UKIC. It also includes any considerations of necessity and proportionality in line with requirements under human rights laws.

There must be a lawful basis in the DPA 2018 for the processing of personal data, which requires at least one of the conditions provided for in Schedule 9 to the DPA 2018 to be met. Further conditions for the processing of sensitive personal data under Part 4 are set out in Schedule 10.

Data subject rights
Chapter 3 ("Rights of the Data Subject") sets out the rights of individuals over their data, including:

- rights to certain general information, including about the processing undertaken by a controller and about data subjects' rights under this Part;
- rights of access by the data subject;

- rights in relation to automated decision-making, including the right not to be subject to such decision-making when it has a significant impact;
- the right to object to processing where the processing would constitute an unwarranted interference with the interests or rights of the data subject;
- the right to rectification of inaccurate data and of erasure of data where the processing of the data would infringe the data protection principles.

As set out below, the DPA 2018 allows for exemption from these rights where it is necessary to safeguard national security. However, this exemption must be applied on a case by case basis and is only available where exemption from specified provisions of Part 4 is required for the purposes of safeguarding national security.

Obligations

Chapter 4 sets out the obligations of controllers (UKIC) and processors (those processing on behalf of UKIC) operating under Part 4 of the Act, to ensure steps are taken so that processing complies with the requirements of Part 4, and that UKIC can demonstrate compliance to the ICO.[11] These obligations include the following sections:

- Data protection by design (Section 103): this provides an obligation on UKIC as a controller to implement the principles of data protection by design, by implementing technical and organisational measures to ensure that the data protection principles are complied with and to minimise risks to the rights and freedoms of data subjects.

- Joint controllers (Section 104): this provides an obligation for joint controllers to determine their respective responsibilities in a transparent manner. To protect the rights of data subjects, joint controller arrangements must ensure there is unambiguous apportionment of the responsibilities provided for in Part 4 of the DPA 2018.

  Two or more intelligence services can operate as joint controllers when they jointly determine the purposes and means of processing. However, UKIC can only enter into a joint controller relationship with each other. UKIC cannot be in a joint controllership relationship with a data controller which is not itself an intelligence service processing under Part 4 of the DPA 2018.

- Processors (Section 105): this provision provides that a controller may only use data processors to process personal data on their behalf if the processor undertakes to implement appropriate measures to comply with the requirements of Part 4 of the DPA 2018, and to provide any information necessary to demonstrate that compliance.

[11] Further details can be found in Part V: Redress

- Security of processing (Section 107): this provision sets out requirements to ensure UKIC and their processors implement appropriate security measures to the processing of personal data. These measures are designed to ensure systems connected with processing are protected from unauthorised processing or interference and requires the implementation of logging systems. This is in addition to the sixth data protection principle that requires appropriate security measures to be implemented.

- Communication of a personal data breach (Section 108): In the event of a data breach which seriously interferes with the rights and freedoms of a data subject or data subjects, the obligation at section 108 requires UKIC, as a controller, to inform the ICO without undue delay. If the report is not made within 72 hours, when it is subsequently provided it must be accompanied by an explanation of the reasons for the delay.

  The duty on a controller is disapplied where the personal data breach also constitutes a relevant error under section 231 of the IPA. This is designed to avoid the double reporting of breaches, whilst ensuring that **all such breaches are subject to independent oversight**. A relevant error under the IPA means an error made by a public authority in complying with any requirement in which the IPC has oversight.

Other Exemptions – Part 4, Schedule 11

In addition to the national security exemption (detailed further below), there are a number of further exemptions provided for at Schedule 11 that permit UKIC to exempt certain provisions of Part 4 in specific circumstances. As with the national security exemption, the need to rely on any of these exemptions must be considered on a case by case basis.

The exemptions listed in Schedule 11 are consistent with those previously available under the DPA 1998. They enable exemption from:

- the Part 4 data protection principles, except for the lawful processing requirement under the first principle and processing must meet a relevant condition that is set out in Schedules 9 and 10;
- the rights of data subjects;
- duties relating to reporting breaches to the ICO.

The exemptions are both prejudice and class based, similar in purpose and effect to several of the exemptions to the GDPR found in Schedule 2 to the DPA 2018 (and those previously provided for under the DPA 1998).

The purpose of the prejudice-based exemptions is summarised below:

- Prevention or detection of crime; apprehension and prosecution of offenders;
- Parliamentary privilege;
- Judicial proceedings;
- The combat effectiveness of the armed forces of the Crown;
- The economic well-being of the United Kingdom;
- Negotiations with the data subject;
- Scientific or historical research, or statistical purposes;
- Archiving in the public interest.

The class-based exemptions requiring specific classes of data to be met are summarised below:

- Information about the conferring of Crown honours and dignities;
- Legal professional privilege;
- Confidential employment, training or education references;
- Exam scripts and marks.

International Transfers

All activities of UKIC must correspond with their statutory functions as set out in the SSA and ISA. This includes the sharing of information, including personal data, with international partners.

International transfers of data by security and intelligence agencies under Chapter 5 of Part 4 of the DPA 2018, meet the requirements of Article 14 of the modernised Convention 108 (C108+) ("Transborder flows of personal data").

Chapter 5 allows for international transfers by security and intelligence agencies where such transfers are necessary and proportionate in order to discharge the statutory functions of the agencies (under the ISA or SSA), or for other purposes specified by relevant parts of those Acts.

Article 14 of C108+ permits transfers of personal data to non-signatory states if "an appropriate level of protection" has or can be secured, or in the following circumstances (Article 14(4)):

(a) where the data subject has explicitly consented (having been informed of the absence of appropriate safeguards);
(b) where *"the specific interests of the data subject require it in the particular case";*
(c) where *"prevailing legitimate interests, in particular important public interests, are provided for by law"*, so long as the transfer is a necessary and proportionate measure in a democratic society; or
(d) on grounds of freedom of expression.

Section H: National Security Data Protection and Investigatory Powers Framework

The underlying premise to the modernised Convention 108 is the recognition that an international transfer should be lawful where it is necessitated by important public interest considerations. Transfers by security and intelligence agencies to international partners are pursuant to security and intelligence agencies statutory functions under the ISA and SSA, so fall within Article 14(4)(c) of the modernised Convention 108.

Additional domestic statutory safeguards on international transfers include the below provisions:

- <u>IPA additional safeguards for international transfers</u>
  The Investigatory Powers Act imposes some specific restrictions that apply to the disclosure to international partners of material obtained under the powers in the Act, which includes personal data.

  Additional safeguards apply to material obtained under interception and equipment interference warrants (both targeted and bulk). This material cannot be disclosed to an international partner unless the person who issued the warrant (the Secretary of State for the intelligence services) is satisfied that that partner applies safeguards to the disclosed material.

  These safeguards should correspond to those in place in the UK (see sections 54, 130, 151 and 192 of the IPA). These should include assurances that an international partner with whom data is shared will:
  a) Only select IPA bulk data for examination for the operational purposes specified in the relevant warrant, and where necessary and proportionate in all the circumstances;
  b) Restrict access to, and copying or dissemination of, IPA data, or intelligence reports based on IPA data, only to the minimum necessary for an authorised purpose;
  c) Retain the data/reports only as long as there is an operational need for it and delete it as long as there are no longer any relevant grounds for retaining it;
  d) Afford additional protections to:
     - The communications, or other information, or UK parliamentarians;
     - Material subject to legal professional privilege;
     - Confidential journalistic material or information that might identify or confirm journalistic sources; and
     - Confidential medical information and confidential spiritual counselling.

- SSA and ISA additional safeguards for international transfers
  ISA and SSA set out the functions of the UKIC agencies, and the purposes for which those functions may be carried out.

  In particular, they place limits on UKIC's collection and disclosure of information, including personal data, so that information may only be disclosed by UKIC if it is necessary for the proper discharge of those statutory functions, in the interests of national security, for the prevention or detection of serious crime, or for the purpose of any criminal proceedings. **These limits apply equally to the disclosure of information to international partners.**

National security exemptions

The DPA 2018 continues the well-established approach to protecting national security and allows for exemption from certain provisions of the Act, applicable where it is necessary to safeguard national security. As a result:

- Section 26 of the Act provides an exemption for national security and defence, which is capable of application to specified provisions of the UK GDPR and DPA 2018, for data controllers/processors operating under that regime.
- Part 3 of the DPA 2018 also provides for national security "restrictions", although this is only relevant to a more limited range of provisions in Part 3.
- Section 110 provides a national security exemption which is capable of application to specified provisions of Part 4 and the wider DPA 2018.

Controllers (including UKIC) **cannot rely** on the national security exemption in relation to the requirement in the first data protection principle for processing to be lawful.

This reflects the approach taken in Convention 108 and is consistent with Article 8 of the ECHR - which requires any interference with the right to privacy to be "in accordance with the law" - and the requirement in section 6 of the Human Rights Act 1998 that public authorities must act compatibly with Convention rights.

Reliance on the national security exemptions in sections 26 and 110 **must be considered on a case-by-case basis** and **is only applicable where exemption from a data protection standard or obligation is necessary to safeguard national security.** Many of the data protection principles and safeguards are consistent with steps already taken by the controllers to protect their data, particularly in the national security context where safeguarding sensitive data is extremely important, so it is not always necessary to exempt processing from all of the data protection principles and obligations.

It is **not enough simply that the data is processed for national security or defence purposes**. A controller must consider the actual consequences to national security or defence if they had to comply with the particular data protection provision and if they could reasonably comply with the usual rule without affecting national security or defence, they must (unless another exemption is applicable).

It is clearly not possible to process data for national security purposes while also complying with all of the data protection obligations.

An example might be where full compliance with the subject access provisions of the DPA 2018 (section 7) would or could inadvertently lead to tipping off a terrorist suspect about an ongoing intelligence investigation. Therefore, to avoid this outcome, it may be necessary to use the exemption to provide a consistent 'neither confirm nor deny' (NCND) response about whether personal data is processed for national security purposes.

This will equally apply to a case where there is no direct impact on national security, so that nothing relating to national security processing can be inferred. This type of NCND response can be applied as a general policy. However, it cannot be applied in a blanket manner: rather, the risk to national security must be considered on a case by case basis.

The national security exemption also specifies provisions within Part 5 (the Information Commissioner) and Part 6 (Enforcement) of the DPA 2018 that can be exempt for the purposes of safeguarding national security. The application of these provisions is explained in Part V of this section.

National Security Certificates

As previously provided for in the DPA 1998, the DPA 2018 enables a controller to apply to a Minister of the Crown (Cabinet Minister, Attorney General or the Advocate General for Scotland) to issue a certificate (under each of the regimes of DPA 2018, section 27, 79 or 111) certifying that a national security exemption or restriction is a necessary and proportionate measure to safeguard national security.

A certificate will continue to be conclusive evidence that an exemption relied upon by the intelligence services from any or all of the specified data protection requirements is required for the purpose of safeguarding national security. It is important to note that a certificate is not required in order to rely on the national security exemption. In fact, in most cases, controllers will determine for themselves whether the national security exemption is applicable. However, national security certificates may provide a controller with greater legal certainty that national security is applicable for specified data processing.

The DPA 2018 also goes further than the DPA 1998, requiring greater transparency over national security certificates. Where a Minister issues a national security certificate under

DPA 2018, he or she is required under section 130 to send a copy to the ICO, who must publish a record of the certificate.

The ICO is required to keep a public record of the certificate, which must include the name of the Minister who issued the certificate, the date on which the certificate was issued and in most circumstances the text of the certificate.

Whilst the expectation is that the requirement to publish a record of a certificate will mean most certificates are published in full, the ICO must not publish the text, or part of the text, of the certificate where the Minister determines that to do so would be against the interests of national security, contrary to the public interest or might jeopardise the safety of a person. In practice, previous certificates have been made available in the public domain and the expectation is that this can continue.

The ICO has published a record of certificates via its website: https://ico.org.uk/about-the-ico/our-information/national-security-certificates. To date the only certificates issued are those to UKIC under sections 27 and 111 of the DPA 2018. The UKIC certificates clearly specify which data protection provisions may be exempt for the purposes of safeguarding national security.

A certificate provides conclusive evidence that certain categories of processing are capable of being exempt on national security grounds. Controllers and processors can only rely on a certificate on a case by case basis when they are seeking to rely on the national security exemption.

PART III: INVESTIGATORY POWERS

Introduction

The IPA introduced world leading oversight arrangements that strengthened the existing safeguards that applied to the use of investigatory powers. It placed these powers on a clear statutory footing, and as set out in the overarching narrative part of this section, ensures that powers are used only when **necessary** for a legitimate purpose and **proportionate** to that purpose.

This part of the document will outline the investigatory powers set out in the IPA. It covers the following:

- Targeted Interception;
- Targeted Communications data;
- Targeted Communications data: internet connection records;
- Targeted Equipment Interference;
- Bulk powers;
- Bulk datasets.

In addition to the above, this part also contains a section on powers under RIPA (obtaining access to protected electronic information), and a section on codes of practice under the IPA.

Each section provides an overview outlining the necessity of the power and lists its key safeguards.

Targeted Interception

Overview

The interception of communications is a vital capability. It is used by law enforcement and UKIC as part of their work to counter serious crime; prevent threats to national security; and protect the interests of the economic wellbeing of the UK, insofar as those interests are also relevant to the interests of national security.

The intercepting authorities will deploy interception by applying for warrants authorised under Part 2 of the Act. Warrants can be issued only when **necessary** for a legitimate purpose and **proportionate** to that purpose. All warrants must be issued by the Secretary of State and approved by a Judicial Commissioner, with the **'double lock'** process acting as a strong safeguard to ensure the necessity and proportionality of the proposed interception activity.

Targeted interception warrants are an investigative tool that enable the interception of communications in relation to a specified subject matter. This may be, for example, an

individual person or a group of persons carrying out a particular activity or sharing a common purpose, such as an organised crime group.

Safeguards

Key limitations and safeguards in relation to this power include the following points:

- The IPA **makes it a criminal offence to intercept the communications of a person in the UK without lawful authority.** It stipulates what constitutes lawful authority to do so.[12] This includes when a targeted warrant has been issued, subject to the conditions in the IPA.
- Only a **strictly limited number of specified public authorities** may request the issuing of such a warrant. These are listed below.
- They can only do so for a **limited range of specified purposes**[13]:
    - where it is necessary in the interests of national security;
    - to prevent or detect serious crime;
    - or in the interests of the economic wellbeing of the UK, insofar as those interests are also relevant to the interests of national security
- The **"double lock"**: this requires all interception warrants to be approved not only by a Secretary of State **but also by a Judicial Commissioner**[14]. This is explained further below in Part IV of this section, including conditions for approval. Both must be satisfied that the warrant is necessary for a legitimate purpose and proportionate to that purpose.
- Requirements that the communications and data obtained from interception is **stored safely**; and that **once no longer required** any information obtained by interception is destroyed. [15]
- **Restrictions on the use or disclosure** of material obtained under interception warrants. This includes an offence for making unauthorised disclosures[16].

[12] Section 6 of the IPA sets out the circumstances in which a person has such "lawful authority". In particular, this is supplemented by Chapter 1 of Part 2, which outlines the conditions for warrants. Chapter 2 also provides for other forms of lawful interception including interception with consent, interception for administrative or enforcement purposes, interception taking place in certain institutions (in prisons, psychiatric hospitals, immigration detention facilities).

[13] Section 20 of the IPA

[14] In urgent cases, it may be issued without prior approval of a judicial commissioner but must then be reviewed within three working days and may be cancelled if the judicial commissioner does not approve it.

[15] Section 53 of the IPA

[16] Sections 53 and 54 provide restrictions for retention and disclosure; section 59 sets out the offence of making unauthorised disclosures.

- Further strong safeguards for such interception relating to members of Parliament, items subject to legal privilege, confidential journalistic material and sources of journalistic information.

The list of public authorities that may apply for the targeted interception powers is contained in section 18 of the IPA. They are:

- The Security Service (MI5);
- The Secret Intelligence Service (SIS);
- Government Communications Headquarters (GCHQ);
- The National Crime Agency;
- The Metropolitan Police Service;
- The Police Service of Northern Ireland;
- Police Scotland;
- Her Majesty's Revenue and Customs; and
- The Chief of Defence Intelligence.

Targeted Communications Data

Overview
Communications data refers to the who, where, when, how and with whom of a telecommunication. It:

- is generated by telecommunications and postal operators in the course of their business practices;
- can include the time and duration of a communication, the number or email address of the originator and recipient, and sometimes the location of the device from which the telecommunication was made;
- does not include the content of any communication, e.g. the text of an email, or what was said on a phone call.

Communications data is an essential tool for law enforcement and national security investigations. It is used to investigate crime, keep children safe, support or disprove alibis and link a suspect to a particular crime scene, amongst many other purposes. It has played an important role in the majority of serious and organised crime and terrorism investigations over the past decade.

Data protection law requires operators to delete data that they no longer require for business purposes. It is therefore necessary to have a power to require the retention of specified data in certain circumstances, given its importance to investigations - where it is

necessary and proportionate to do so. If data is not retained, it cannot be accessed subsequently.

The IPA therefore provides for the acquisition and retention of communications data in Parts 3 and 4 respectively[17]. Part 4 stipulates that telecommunications and postal operators may be required by the Secretary of State to retain communications data and enables communications data to be retained for up to 12 months, subject to strict limitations and safeguards. It does not require them to retain the content of the communication.

Safeguards

Key limitations and safeguards in relation to this power include the following points:

- When acquiring events data (the more intrusive communications data) for the prevention or investigation of crime, **the serious crime threshold must be met**.[18] A retention notice can only be issued by the Secretary of State where the relevant information has been considered (e.g. the size of the telecommunications operator or postal operator), and it is considered **necessary and proportionate** to do so for a limited range of purposes, set out below;
- A retention notice can only be issued where it has been approved by a Judicial Commissioner[19], who must review the Secretary of State's conclusions about the necessity and proportionality of the notice;[20]
- All retention notices are **reviewed annually** (as well as informally on an ongoing basis) to ensure they continue to meet the necessary and proportionate requirements. Requirements for the telecommunications operators and postal operators under a retention notice to ensure that retained data is **stored securely, with access controls**, as set out in Section 92 of the IPA.
- **Only a strictly limited number** of **specified public authorities** can apply for communications data. These are specified in Schedule 4 to the IPA and include the law enforcement agencies and UKIC.
- The authorities may only acquire communications data where it is both **necessary and proportionate to do so for specified purposes**. These are set out below.

[17] Part 3 of the IPA provides the statutory framework governing the acquisition of communications data by public authorities, and its disclosure by telecommunications or postal operators. Part 4 of the IPA sets out the provisions for the retention of communications data, so it is available for subsequent access by public authorities when authorised under the appropriate provision.

[18] This threshold is offences which would attract a one-year sentence. This is set out in section 87 of the IPA, as amended by the Data Retention and Acquisitions Regulations 2018

[19] In urgent cases, it may be issued without prior approval of a judicial commissioner but must then be reviewed within three working days and may be cancelled if the judicial commissioner does not approve it.

[20] Sections 87 and 89 of the IPA

- An applicant must **complete a stringent application process**, including setting out the necessity and proportionality considerations. A communications data code of practice sets out the considerations regarding necessity and proportionality.
- The vast majority of applications for communications, except in urgent or national security scenarios, will be required to be independently authorised by the Office for Communications Data Authorisations (OCDA).
- Where an application for communications data is for the purpose of national security or where it is an application made by a member of an agency under section 61(7)(b), an application may be authorised internally by a designated senior officer in a public authority.
- A designated senior officer is a person holding a prescribed office or rank in a relevant public authority who is responsible for authorising certain applications where the requirement for independent authorisation does not apply.

  Those individuals who undertake the role of authorising individual must have current working knowledge of human rights principles and legislation, specifically those of necessity and proportionality, and how they apply to the acquisition of communications data under Part 3 of the Act and the Communications Data Code of Practice.

  The designated officer must, except where provided for in the Act, be independent of the operation concerned.

  A designated senior officer may also authorise a request for communications data where there is an urgent need to acquire the data because of an imminent threat to life or another emergency.
- A code of practice, providing more detail on access to communications data. Its effect is set out in Paragraph 6 of Schedule 7 to the IPA. A person must have regard to the codes when exercising any functions to which the codes relate. The codes are admissible as evidence and a court or tribunal may take into account a failure to have regard to them.
- Furthermore, the use of communications data is subject to the **oversight of the IPC** who ensures adherence to the policies and processes described in the code of practice. This is further outlined in Part IV of this document ("Oversight").

As mentioned above, the acquisition of communications data must be for at least one of the operational purposes listed under the IPA. These are:

- in the interest of national security;
- for the purpose of preventing or detecting crime or of preventing disorder;

- in the interest of the economic well-being of the United-Kingdom so far as those interests are also relevant to the interests of national security;
- in the interests of public safety;
- for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health;
- to assist on the miscarriages of justice;
- to assist investigations into alleged miscarriages of justice; or
- where a person (P) has died or is unable to identify themselves because of a physical or mental condition to a) assist in identifying P, or b) to obtain information about P's next of kin or other persons connected with P or about the reasons for P's death or condition.

Targeted Communications Data: Internet Connection Records

Overview

Internet Connection Records (ICRs) are a type or subset of communications data. An ICR is a record comprised of a number of items of communications data of the service to which a customer has connected to on the internet. An example of an ICR is a website or instant messaging application.

An ICR is not a person's full internet browsing history. It is a record of the services that they have connected to. These can be vital to investigations such as identifying an individual who has accessed a website containing child sexual abuse imagery, or identifying which unlawful websites an individual has accessed, such as sites hosting child sexual abuse imagery. It would not reveal every web page within a website that someone has visited or anything that they do on a web page.

An ICR is captured by the company providing access to the internet. Where available, this data may be acquired from communication operators by law enforcement and UKIC. ICRs are **vital to law enforcement investigations** in a number of ways. For example:

- To assist in identifying who has sent a known communication online, which often involves a process referred to as internet protocol (IP) address resolution;
- To establish what services a known suspect or victim has used to communicate online, allowing investigators to request more specific communications data;
- To establish whether a known suspect has been involved in online criminality, for example sharing indecent images of children, accessing terrorist material or fraud;
- To identify services a suspect has accessed which could help in an investigation including, for example, mapping services.

The Communications Data Code of Practice sets out the further safeguards which apply to ICR retention and acquisition, which are in addition to the stringent safeguards applicable to all requests for communications data (set out in the targeted communications data section).

If ICRs are sought for the investigation of crime, where the list of the records will be disclosed, the serious crime threshold must be met in all circumstances. Local authorities cannot acquire ICRs for any purpose.

Targeted Equipment Interference

Overview

Equipment interference (EI) is a set of techniques used to obtain a variety of data from equipment. The definition of "equipment" includes traditional computers or computer-like devices such as tablets, smart phones, and static storage devices.

Equipment interference provides operational benefits in relation to the investigation of crime in two ways:

- Firstly, as a stand-alone capability, working in conjunction with other intelligence gathering, it provides insight, intelligence, investigative and evidential opportunities in to a suspect's life.
- Secondly, when combined with other warranted investigative powers, such as interception, it provides a wider range of tools to access the communications of criminals that might otherwise be out of reach of traditional interception.

Section 13 and 14 and Part 5 of the IPA cover targeted equipment interference powers.

Safeguards

Key limitations and safeguards in relation to this power include the following points:

- UKIC, defence intelligence, and law enforcement agencies (LEAs) listed in Schedule 6 to the IPA may apply for a targeted equipment interference warrant. For law enforcement, this includes the police, the National Crime Agency, Her Majesty's Revenue and Customs (HMRC) and immigration officers.
- The IPA applies strong safeguards by ensuring that equipment interference is used only when **necessary** for a legitimate purpose and **proportionate** to that purpose.
- The **"double lock"**: this requires all equipment interference warrants to be approved not only by a Secretary of State or a law enforcement chief, **but also by a Judicial**

Commissioner[21]. Both must be satisfied that the warrant is necessary for a legitimate purpose and proportionate to that purpose[22]. This is explained further below in Part IV of this section, including conditions for approval.

- Requirements that the data obtained from equipment interference is **stored safely**; and that any information obtained from equipment interference is destroyed **as soon as there are no longer any grounds** for retaining it. Warrants are reviewed every 6 months (unless urgent) and appropriate safeguards are in place where material has been obtained under an EI warrant.[23]

- For the purpose of the intelligence services, a warrant can be issued if it is necessary in the interests of national security, for the purpose of preventing or detecting serious crime, and/or in the interests of the economic well-being of the UK, so far as those interests relate to national security. For Defence Intelligence, the warrant must be necessary in the interests of national security.

- For law enforcement agencies, the warrant must be necessary for the purpose of preventing or detecting serious crime. For certain law enforcement agencies[24], a warrant can also be issued if it is necessary on the grounds of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health. [25]

- Further safeguards for the acquisition of material relating to members of Parliament, items subject to legal privilege, confidential journalistic material and sources of journalistic information.

- Furthermore, section 107 of the IPA places restrictions on the issue of EI warrants for law enforcement. Specified LEAs may only be issued with a targeted EI warrant if there is a British Islands connection. This includes warrants issued to a member of a police force listed in section 2 of Police Act 1996, the Metropolitan Police, MoD police, Police Investigations and Review Commissioner, Independent Office of Police Conduct, British Transport Police, Police Service Scotland or Police Service Northern Island. In contrast, LEAs not listed at section 107(2) such as the NCA are permitted to apply for EI warrants for operations outside the UK.

A British Islands connection as mentioned above exists if:

[21] In urgent cases, it may be issued without prior approval of a judicial commissioner but must then be reviewed within three working days and, where a judicial commissioner refuses to approve a decision, anything being done under the EI warrant must stop as soon as is reasonably practicable.
[22] Sections 102-104 and 106 of the IPA
[23] Section 129-133 of the IPA
[24] Listed in Part 1 of Schedule 6 to the IPA
[25] Use of EI for these additional purposes will only be used in exceptional circumstances, with it most likely being used to assist in locating vulnerable persons. As a result, only a limited number of LEAs can apply for EI for these purposes (listed in Part 1 of Schedule 6 to the IPA).

- Any of the conduct authorised by the warrant would take place in the British Islands, regardless of the location of the equipment that would, or may, be interfered with;
- Any of the equipment which would, or may, be interfered with would, or may, be in the British Islands at some time whilst the interference is taking place; or
- A purpose of the interference is to obtain:
    - Communications sent by, or to, a person who is, or whom the law enforcement officer believes to be, for the time being in the British Islands;
    - Information relating to an individual who is, or whom the law enforcement officer believes to be, for the time being in the British Islands; or
    - Equipment data which forms part of, or is connected with, communications or information falling within the above.

To further ensure that EI activity conducted by these agencies are focussed on investigations or operations within the British Islands, irrespective of whether there is a British Islands connection, they are prohibited by the EI code of practice, from obtaining an EI warrant for interferences that take place outside of the British Islands, unless:

- the subject of the investigations is a UK national;
- the subject of the investigations is likely to become the subject of criminal or civil proceedings in the UK;
- the operation is likely to affect a UK national; or
- the operation is likely to give rise to material likely to be used in evidence before a UK court.

Bulk Powers

Overview

This section deals with powers to acquire bulk data under the IPA. Bulk personal datasets are dealt with in the section below.

The IPA established a clear statutory framework for the bulk powers available to UKIC, providing robust, consistent safeguards across all of those powers. Bulk powers may only be sought by UKIC and must be **necessary** and **proportionate** and in the **interests of national security.**

The threats to the UK are diverse and constantly evolving. Technological changes have transformed the challenge facing UKIC. Terrorists and criminals have embraced social media and online spaces to radicalise, recruit, inspire, plan, coordinate and increasingly to execute their attacks and other activities. Evolving technology, including more widespread use of the internet and ever-more internet-connected devices, stronger encryption and cryptocurrencies, continue to create challenges in fighting terrorism.

In this context, and given data is more dispersed, localised and anonymised, and increasingly accessible from anywhere globally, bulk powers have proved essential to UKIC over the last decade and will be increasingly important in the future to identify threats that cannot be identified by other means. Conventional targeted techniques are insufficient on their own to deal with the range of threats both online and in contexts where the UK does not have presence on the ground.

In addition to this, bulk powers allow UKIC to identify and map out known and evolving networks. They enable UKIC to identify new threats, wider networks, attack planning and threats overseas.

Within the UK itself, the analysis of bulk communications data or bulk personal datasets is often the only way for UKIC to progress investigations and identify terrorists from very limited lead intelligence, or when their communications have been deliberately concealed.

There are a number of similarities between the conduct that Bulk and Targeted Thematic warrants can authorise.[26] The key factor that determines whether an activity should be authorised under a Targeted Thematic or Bulk warrant is foreseeability. If the agency is able to foresee the extent of all of the proposed activity to a sufficient degree at the time of seeking a warrant, then a Targeted Thematic warrant may be granted.

However, there may be instances in which it is not possible to foresee the extent of all the proposed activity and in these cases a Targeted Thematic warrant may not be appropriate. In such circumstances, UKIC can apply for a Bulk warrant, which provide for additional safeguards.

Bulk Powers provided for in the IPA

The IPA established a clear statutory framework for the bulk powers available to the UKIC, providing **robust, consistent safeguards** across all of those powers. The following bulk powers are provided for in Part 6 of the IPA[27]:

- Bulk interception (Part 6, Chapter 3) is the interception of overseas-related communications and the subsequent selection for examination of the intercepted material. Bulk interception is an intelligence gathering tool that is used, for example, to identify previously unknown threats to the national security of the UK.

[26] Thematic warrants can be obtained for targeted equipment interference and targeted interception. A thematic warrant is used where, in the context of equipment interference, the equipment is linked by a common theme. A thematic warrant can cover a wide range of activity, or a wide geographical area, or involve the acquisition of a significant volume of data (see for example sections 101(1)(b), (c), and (e) to (h), and 101(2)(b) to (e)).

[27] Bulk interception is set out in Chapter 1 of Part 6; bulk communications data in Chapter 2; bulk equipment interference in Chapter 3.

Bulk interception is essential because UKIC frequently have only small fragments of intelligence, or early, not fully developed leads about people overseas who pose a threat to the UK. UKIC are able to filter and analyse bulk interception material in order to identify communications of intelligence value. Often the data acquired via bulk interception is the only way UKIC can gain insight into particular areas and threats. Bulk interception may be used, for example:

- to establish links between known subjects of interest, improving understanding of their behaviour and the connections they are making or the multiple communications methods they may be using;
- to search for traces of activity by individuals who may not yet be known but who surface in the course of an investigation, or to identify patterns of activity that may indicate a threat to the United Kingdom.

- Bulk communications data (Part 6, Chapter 2) refers to the acquisition of communications data in bulk from a telecommunications operator. The ability to acquire and access this data in bulk, subject to strict safeguards and oversight, is vital to their effectiveness, providing unique intelligence that cannot be obtained by other means.

  It is essential to enable communications relating to subjects of interest to be identified and subsequently pieced together in the course of an investigation. In some cases, bulk communications data may be the only investigative resource with which UKIC have to work. The analysis of bulk communications data has played an important part in every major counter terrorism investigation of the last decade.

- Bulk equipment interference (Part 6, Chapter 3) describes a set of techniques to obtain information from devices that are necessary for the identification of subjects of interest who pose a threat to the UK's national security, in circumstances where the information is not available through the use of other methods.

  It refers to the acquisition of overseas related-communications, equipment data and information described in the warrant and/or to select for examination of such material. **Bulk equipment interference warrants can only be issued to the intelligence services**.

Bulk warrants will usually only be appropriate for large scale operations and are only available for operations for the obtaining of overseas related communications, overseas related information or overseas related equipment data.

When determining whether a targeted or bulk warrant is appropriate, regard must be given to whether the Secretary of State is able to foresee the extent of all of the interferences to a

sufficient degree to properly and fully assess necessity and proportionality at the time of issuing the warrant.

Bulk powers are not indiscriminate and can only be used where it is necessary and proportionate to do so, as with other powers. UKIC are always required to operate in accordance with **strict safeguard**s and under **parliamentary, independent judicial and ministerial oversight.** These are further set out below.

With reference to bulk interception, the Chamber of the ECtHR made the following consideration in *Centrum för rättvisa v. Sweden*:

> *"Given the reasoning of the Court in those [previous] judgments and in view of the current threats facing many Contracting States (including the scourge of global terrorism and other serious crime, such as drug trafficking, human trafficking, sexual exploitation of children and cybercrime), advancements in technology which have made it easier for terrorists and criminals to evade detection on the internet, and the unpredictability of the routes via which electronic communications are transmitted, the Court considers that the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States' margin of appreciation."*

In addition to this, Lord Anderson QC conducted an independent review into whether the operational case for bulk powers in 2016 had been made (see supplementary material). The government provided complete access to the most sensitive information to enable the review to be undertaken effectively.

This review, which also looked at the agencies' use of bulk personal datasets, significantly underlined the development of bulk powers because his review team critically appraised the need for bulk capabilities. This included considering whether the same result could have been achieved through alternative investigative methods. The review noted that *"where alternative methods exist, they are often less effective, more dangerous, more resource-intensive, more intrusive or slower."*[28]

The report made absolutely clear the critical importance of bulk powers to UKIC. It concluded that:

- "*The bulk powers play an important part in identifying, understanding and averting threats in Great Britain, Northern Ireland and further afield.*"[29]

[28] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF, p. 102
[29] Ibid, p. 1.

- Bulk interception is of "*vital utility*" to UKIC and that alternative methods fall short of providing the same results. In one case assessed by the review team, in which a kidnap had taken place in Afghanistan, the report finds that: "*Without the use of bulk interception, it was highly likely that one or more of the hostages would have been killed before a rescue could be attempted.*"[30]

- Bulk acquisition of communications data is "*crucial in a variety of fields, including counter-terrorism, counter-espionage and counter-proliferation*"[31] and its use cannot be matched by data acquired through targeted means. Case studies provided to the review demonstrated that: "*bulk acquisition has contributed significantly to the disruption of terrorist operations and, through that disruption, almost certainly the saving of lives.*"[32]

- An operational case for bulk equipment interference has been made in principle and there are likely to be cases where "*no effective alternative is available.*"

On the concern that bulk capabilities may be used to conduct 'mass surveillance', Lord Anderson concluded that:

> *"Whether a broader or narrower definition is preferred, it should be plain that the collection and retention of data in bulk does not equate to so-called "mass surveillance"*[33]*. Any legal system worth the name will incorporate limitations and safeguards designed precisely to ensure that access to stores of sensitive data is not given on an indiscriminate or unjustified basis. Such limitations and safeguards certainly exist in the [Investigatory Powers] Bill."*[34]

In addition to this, Lord Anderson listed multiple occasions when the bulk powers have saved lives, averted terrorist attacks, and allowed children to be saved from sexual abuse and exploitation.

Safeguards

Key limitations and safeguards include the following points:

- Bulk powers can only be used when a warrant has been issued and the use of bulk warrants is **limited to UKIC.**

[30] Ibid, p. 85.
[31] Ibid, p. 102.
[32] Ibid, p. 102.
[33] The UK's Intelligence and Security Committee of Parliament, independent commissioners and the Investigatory Powers Tribunal have confirmed in detailed reports and judgments that UK agencies neither conduct, nor seek to conduct, mass surveillance.
[34] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF, p. 4.

- Warrants for the use of these powers are only issued where it is both **necessary and proportionate** to do so:
    - **At least one of the grounds** for issuing a bulk interception, bulk communications data, or bulk equipment interference warrant must always be that the warrant is **necessary in the interests of national security**. It may also include a further purpose of preventing or detecting serious crime; or in the interests of the economic wellbeing of the UK so far as those interests are also relevant to the interests of national security.
    - Each warrant must be **clearly justified and balance** intrusions into privacy against the expected intelligence benefits.
- The **'double lock'**: all warrants must also be approved by a Judicial Commissioner[35], who must review the Secretary of State's conclusions about the necessity and proportionality of the notice.
- Bulk warrants must also specify the more detailed **operational purposes** for which material acquired under those warrants may be examined. An operational purpose may not be specified on an individual bulk warrant unless it is a purpose that is specified on the central list maintained by the heads of the UKIC agencies.

  The central list of operational purposes must be approved by the Secretary of State, reviewed on an annual basis by the Prime Minister, and shared every three months with the Intelligence and Security Committee.
- Selection for examination of any data acquired and retained under a warrant must always be necessary and proportionate for at least one of the operational purposes specified on the warrant.
- A **record of the reasons** why it is necessary and proportionate to examine bulk data for the applicable operational purpose(s) must be created before the data is examined. These records must by retained by UKIC and are subject to **external audit by IPCO.**
- Deliberate selection for examination of bulk data in breach of the safeguards of the IPA has been **made a criminal offence** and may be subject to criminal prosecution[36].
- Further guidance on how the necessity and proportionality tests must be applied in practice is provided in **the Codes of Practice** published alongside the IPA.

[35] In urgent cases, it may be issued without prior approval of a judicial commissioner but must then be reviewed within three working days and may be cancelled if the judicial commissioner does not approve it.
[36] Sections 155, 173, and 196 of the IPA

Additional bulk power safeguards for people located in the British Islands

Within the British Islands, the targeted interception of communications is a tool used to advance investigations into known threats, usually in conjunction with other capabilities, such as surveillance or agent reporting.

By contrast, bulk powers are often the only means available to discover threats outside the British Islands, particularly in countries where investigating agencies might have no physical presence at all.

In those circumstances, it will often be necessary to examine the communications of individuals outside of the British Islands that have been obtained under a bulk interception or bulk equipment interference warrant. This examination may be based on partial intelligence in order to determine whether the individuals merit sustained investigation. The **ability to do this is crucial to mitigating threats to the UK from overseas.** This examination will be subject to consideration of necessity and proportionality, and **to the bulk data examination safeguards set out above.**

On occasion, it may be necessary to examine the content of communications of a person in the British Islands that have been obtained under a bulk interception or bulk equipment interference warrant. Except in strictly time-limited circumstances, UKIC must first obtain a targeted examination warrant in relation to that person in order to carry out such examination.

Applications for targeted examination warrants will be supported by a detailed intelligence case that allows the Secretary of State to satisfy him or herself that this use of investigatory powers is appropriate, and are required to meet the same standards of necessity and proportionality and are subject to the same double lock procedure of approval by a Judicial Commissioner as targeted interception or target equipment interference warrants.

In the case of *Big Brother Watch and others v the United Kingdom*[37], the ECtHR specifically considered the issue of whether it was appropriate to maintain different safeguards based on an individual's location and concluded:

> "*the exclusion of communications of individuals known currently to be in the British Islands is, in the opinion of the Court, an important safeguard, since persons of interest to the intelligence services who are known to be in the British Islands could be subject to a targeted warrant under section 8(1) of RIPA. The intelligence services should not be permitted to obtain via a bulk warrant what they could obtain via a targeted warrant*."

[37] 58170/13 62322/14 24960/15

Bulk Personal Datasets

Overview

In the context of the IPA, a bulk personal dataset (BPD) is a set of data that includes personal information relating to a number of individuals, such as the electoral roll or telephone directories. The majority of these individuals are unlikely to become of interest to UKIC.

The agencies use BPDs to fulfil their statutory functions, including protecting national security. BPDs are essential in helping UKIC to identify subjects of interest or individuals who surface during the course of an investigation, to better understand a subject of interest's behaviour and connections, and to quickly exclude innocent individuals from further inquiries. The Anderson report noted that BPDs are of great utility to UKIC and in vital areas of work, where there is "*no practicable alternative*".

BPDs are acquired through overt and covert means and in accordance with the SSA and the ISA. BPDs may be acquired using investigatory powers, from other public-sector bodies or commercially from the private sector. These datasets are typically very large, and so need to be processed electronically.

The provisions of the IPA relating to BPDs **do not create a power to acquire data in bulk**. Part 7 of the IPA allows such datasets to be retained and examined by UKIC where it is necessary and proportionate to do so. It creates two types of BPD warrant – class BPD warrants and specific BPD warrants:

- Class BPD warrants authorise the retention of a class of BPDs, such as certain kinds of travel datasets that relate to similar routes and which contain information of a consistent type and level of intrusiveness.

- Specific BPD warrants authorise the retention of a specific dataset – this could be because the dataset is of a novel or unusual type of information so does not fall within an existing class BPD warrant, or because a dataset raises particular privacy concerns that should be considered separately.

Safeguards

The IPA sets out an additional set of statutory restrictions and safeguards, over and above the safeguards in Part 4 of the Data Protection Act 2018.

Key limitations and safeguards include the following points:

- Following a strictly time-limited period of initial examination to determine whether it is necessary and proportionate to retain a BPD, BPDs **can only be retained, or retained and examined by UKIC when a warrant** has been issued.[38]

[38] Section 200 of the IPA.

- Warrants for the retention, or retention and examination of bulk personal datasets are only issued by the Secretary of State where it is both **necessary and proportionate** to do so[39]:
    - Each warrant must be necessary for at least one of these grounds:
        - in the interests of national security;
        - the purpose of preventing or detecting serious crime; or
        - in the interests of the economic wellbeing of the UK so far as those interests are also relevant to the interests of national security.
    - Each warrant must be clearly justified and balance intrusions into privacy against the expected intelligence benefits.
- Warrants cannot be issued unless the Secretary of State is satisfied with UKIC's arrangements for storing the BDP and protecting it from unauthorised disclosure.
- The **"double lock"**: all BPD warrants must also be approved **by a Judicial Commissioner**, who must review the Secretary of State's conclusions about the necessity and proportionality of the notice. This is explained further below in Part IV of this document, including conditions for approval.
- A **record of the reasons** why it is necessary and proportionate for the applicable operational purpose(s) must be created before the data is selected for examination. These records must be retained by UKIC and are subject to **external audit by IPCO**.
- Deliberate selection for examination of bulk data in breach of the safeguards of the IPA has been made a **criminal offence** and may be subject to criminal prosecution[40].

Part III Regulation of Investigatory Powers Act (RIPA)

Overview

Information security technologies have allowed electronic commerce to flourish, enabling businesses and individuals to secure and protect their electronic data and to maintain the privacy of their electronic communications. Individuals going about their lawful business, openly and privately, use these technologies every day.

Terrorists and criminals use the same technologies to protect their electronic data and the privacy of their electronic communications, to conceal evidence of their unlawful conduct and to evade detection and prosecution.

[39] Sections 204 and 205 contain the necessity and proportionality requirements for class and specific BPDs respectively. Further guidance on how the necessity and proportionality tests must be applied in practice is provided in the Codes of Practice published alongside the IPA

[40] Section 224 of the IPA

Protected electronic information means any electronic information that cannot be readily accessed or put into intelligible form without a key. A key means any key, password, algorithm or other data which allows access to the information or allows it to be put into an intelligible form. Access to protected electronic information is vital, and among other things, provides public authorities with the tools they need to gather evidence for the purpose of court proceedings.

Section 49 of RIPA Part III applies where **protected electronic information** has come into the possession of any person by means of a statutory power to seize, detain, inspect, search or otherwise interfere with documents or property.

The provisions in Part III provide a statutory framework for public authorities to require protected information which they have obtained lawfully or are likely to obtain lawfully be put into an intelligible form; to acquire the means to gain access to protected information and to acquire the means to put protected information into an intelligible form.

Section 49 thus provides a power to require disclosure of protected information in an intelligible form.[41]

Safeguards

- The powers under RIPA Part III **may only be exercised by a person holding "the appropriate permission.**" For the purpose of Section 49, "the appropriate permission" can only be sought from a judge. However, depending on the circumstances of how the information came into the possession of a public authority and who is seeking permission, it may be possible to seek permission via other routes. For example, if the information was obtained under a warrant approved by the Secretary of State, then the Secretary of State would need to approve the giving of the notice.

- A notice may be given where a person who has appropriate permission, reasonably believes that:

    a. a key to the protected material is in possession of any person;

    b. a disclosure requirement in respect of the protected information is **necessary** in the interests of national security, for the purpose of preventing or detecting crime, in the interests of the economic well-being of the UK so far as those interests are also relevant to the interests of national security, or for

[41] Further powers are laid down in Section 50(3) - power to require disclosure of the means to access protected information or of the means of putting protected information into an intelligible form (section 50(3)(c)). The power to attach a secrecy provision to any disclosure requirement is set out in section 54.

the purpose of securing the effective exercise or proper performance by any public authority of any statutory duty

c. such a requirement is **proportionate** to what is sought to be achieved by its imposition; and

d. that it is not reasonably practicable for the person with the appropriate permission to obtain possession of the protected information in an intelligible form without the giving of a notice.

- Further safeguards are set out in section 55 of RIPA. Every person whose officers or employees include persons with duties that involve the giving of section 49 notices must ensure arrangements are in place so that:
    - the use and retention of keys are proportionate to the aim;
    - keys are stored in a secure manner; and
    - all records of keys are destroyed as soon as they are no longer necessary.
- Investigators must take into account the legitimate needs of businesses and individuals to maintain the integrity of their information security management processes.
- Where the powers and duties under RIPA Part III are not already being exercised by or with the permission of an independent judicial authority, independent oversight is carried out by the IPC. Persons exercising these powers must adhere to the practices and processes described by the code of practice. Complaints about the giving of a notice can be made to the Investigatory Powers Tribunal.

Examples of such information include requiring a suspect to divulge the password to a social media account or the PIN to a locked smartphone if the police have reasonable grounds for believing that person has the password or PIN in their possession, and it is not reasonably practicable to obtain access to the information without the giving of a notice.

Codes of Practice

The IPA and other legislation governing the use of investigatory powers is accompanied by a set of statutory Codes of Practice which explain how the powers can be used.

These codes, which are subject to public consultation and must be scrutinised and formally approved by both Houses of Parliament, set out further detail on the processes and safeguards for the use of investigatory powers by public authorities.

The codes are updated when necessary. The most recent set of codes were published and updated in 2018, and cover the bulk acquisition of communications data, UKIC's retention and use of bulk personal datasets, equipment interference, interception of communications,

national security notices, and communications data. The most recent versions of the codes can be accessed at:

- https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice
- https://www.gov.uk/government/collections/ripa-codes#current-codes-of-practice

The IPA provides that all codes of practice issued under Schedule 7 are admissible as evidence in criminal and civil proceedings.

If any provision of one of these codes appears relevant to any court or tribunal considering any such proceedings, the Investigatory Powers Tribunal, the IPC, or to the Information Commissioner, it may be taken into account.

The duty placed upon public authorities, including law enforcement and UKIC, to have regard to the Code when exercising functions to which the Code relates exists regardless of any contrary content of an authority's internal advice or guidance.

Each Code of Practice follows a similar format setting out, among other things:

- Relevant definitions and how those definitions apply in respect of the relevant power;
- Guidance on general considerations around necessity and proportionality;
- The processes for seeking a warrant or authorisations, including details on roles and responsibilities, duration, review/renewal and guidance on the processes to be followed in urgent cases;
- Guidance on acquiring data in relation to those who handle sensitive information;
- Guidance on compliance by telecommunications operators and relevant offences;
- Safeguards around retention and use of data obtained under the powers, including, for those Codes covering bulk powers, guidance on selection for examination; and
- Guidance on costs, record keeping and oversight.

PART IV: OVERSIGHT

Overview

The use of investigatory powers by UKIC and other public authorities is subject to a comprehensive regime of overlapping executive, legislative and judicial oversight that is arguably unmatched anywhere in the world.

These key elements include the following points:

- The functions of UKIC and the purposes for which they may exercise those functions, are set out in statute. The head of each agency is **accountable to a Secretary of State** for the proper discharge of the agency's functions.
- As noted already, under the IPA and related legislation (including Part II of RIPA), the Secretary of State must also **personally approve the exercising by the Agencies of all the more intrusive investigatory powers**. This includes the interception of communications and equipment interference by issuing warrants authorising the activity.
- Codes of Practice under the IPA set out in considerable detail the information that must be provided by an agency when seeking a warrant, and also **the matters that the Secretary of State must consider when deciding** whether or not to issue the warrant. In discharging his or her responsibilities, the Secretary of State is additionally subject to the long-established Ministerial Code, which sets out the standards of conduct expected of Ministers and how they discharge their duties.
- IPA warrants issued by the Secretary of State are subject to the **double lock**: They must be approved by an independent Judicial Commissioner, under the auspices of the IPC, before they can be issued.
- IPC is also responsible for **post hoc oversight** of the activities of the agencies and is assisted in this function by the Judicial Commissioners, by a team of experienced inspectors, and by a panel of technology advisers. The IPC is also obliged to make an **annual report** to the Prime Minister on the use of investigatory powers under the IPA. This report must be published and laid before Parliament.
- The policy, administration and expenditure of the three Agencies is also subject to oversight by the **Intelligence and Security Committee of Parliament (ISC)**. The ISC has the power to conduct retrospective oversight of the UKIC's operational activity and to examine the wider intelligence and security activities of Government. Members of the ISC are appointed by Parliament and the Committee reports directly to Parliament.

The activities of UKIC are also subject to **challenge from the Information Commissioner (ICO), Courts, and Tribunals including before the IPT**. This is set out in Part V (Redress).

This section describes the key elements of the oversight regime, addressing:

i. Independent Judicial Oversight;
ii. Parliamentary Oversight; and
iii. Transparency Reporting.

Independent Judicial Oversight: Investigatory Powers Commissioner

Overview

The use of investigatory powers by UKIC and other public authorities is subject to independent judicial oversight by the IPC, and 15 Judicial Commissioners working under the IPC.

This includes the **"double lock"** where use of intrusive powers must be agreed both by senior officers or the Secretary of State, and by a Judicial Commissioner.

The IPC covers all investigatory powers and is responsible for reviewing warrants issued for the interception of communications and functions previously carried out by the Intelligence Services Commissioner. This includes reviewing warrants issued to authorise intrusive surveillance and interference with property.

Lord Justice Sir Adrian Fulford was appointed as the first IPC in February 2017 by the Prime Minister under section 227(1) of the Investigatory Powers Act 2016. The current IPC is Sir Brian Leveson (appointed October 2019); a senior judicial figure who was formerly the President of the Queen's Bench Division of the High Court and Head of Criminal Justice.

Role and Powers

The IPC's main oversight functions are extensive and detailed in legislation (see s229 and 230 of the IPA). This includes responsibility for keeping under review (including by way of audit, inspection and investigation) the exercise by public authorities of statutory functions relating to:

- the interception of communications;
- the acquisition or retention of communications data;
- the acquisition of secondary data or related systems data;
- equipment interference;
- surveillance;
- error reporting, and
- broader UKIC oversight.

The IPC and Judicial Commissioners are supported in their roles by the Investigatory Powers Commissioner's Office (IPCO). IPCO has a significantly expanded staff compared to its predecessor organisations, including a team of inspectors, in-house legal and technical expertise, and a Technology Advisory Panel to provide expert advice.[42]

The IPC and Judicial Commissioners are also responsible for approving decisions by Secretaries of State, Scottish Ministers and senior officials in law enforcement to authorise warrants applied for under the Investigatory Powers Act. These warrants include:

- Targeted interception and bulk interception warrants;
- Targeted equipment interference and bulk equipment interference warrants;
- Bulk personal dataset warrants;
- Bulk acquisition of communications data warrants;
- Targeted examination warrants; and
- Mutual assistance warrants.[43]

The 'double lock' means that the Commissioner must review the decision to issue a warrant and consider whether it is necessary for the purpose stated and proportionate to what is expected to be achieved. **If the Judicial Commissioner is not satisfied on these points, the warrant cannot be issued and no action authorised by it can be taken**. The government may appeal to the IPC, but his decision is final.

Warrants are typically granted for six months. If the warrant is to be renewed, then it must go through the 'double lock' again. This will include a review of what intelligence product has been gathered and what collateral intrusion into the privacy of third parties has occurred.

The law allows that in an urgent case, a warrant can be issued before being approved by a Judicial Commissioner[44]. However, within three working days of the issuing, the Commissioner must then consider whether to approve both the decision to issue, and the decision to use the urgent process. If the warrant is not approved by the Commissioner, it ceases to have effect and cannot be renewed.

[42] The panel's role is set out on the IPCO website and in legislation at s246 of the IPA and includes advising the IPC on: (a) the impact of changing technology on the exercise of investigatory powers whose exercise is subject to review by the Commissioner, and (b) the availability and development of techniques to use such powers while minimising interference with privacy.
[43] A Mutual Assistance Warrant is an interception or other warrant issued in response to a request from a foreign government, rather than from a UK agency.
[44] This is set out in section 24 and 25 of the IPA.

Published Guidance and Public Consultation

IPCO is committed to being open and transparent, within the limits of the law and the constraints of the subject matter with which they deal. As part of this commitment to openness, they have published an 'Advisory Notice on the Approval of Warrants, Authorisations and Notices by Judicial Commissioners' [see supplementary material], following extensive discussions with the Judicial Commissioners.

This Notice has been agreed in order to provide a guide as to how the Judicial Commissioners approach the information available to them when deciding whether to approve or refuse the Secretary of State's decision to issue a warrant under IPA. This is to ensure there is a clear understanding as to how the Commissioners undertake this important task.

IPCO also launched a consultation exercise aimed at identifying the broad range of factors that the Judicial Commissioners should have in mind, and the approach they should take to the various competing considerations that are relevant to their approval of bulk warrants. They have invited a range of NGOs to consider two questions:

- What factors should the Judicial Commissioners take into account when considering whether the conduct proposed in a bulk warrant is proportionate? and
- Is there any particular approach that the Commissioners should adopt when evaluating those factors, some of which may be competing?

IPCO has considered the submissions received in response to its public consultation on the use of bulk powers as set out in the IPA. These have been reviewed by independent standing counsel and discussed with the Judicial Commissioners.

Its 2017 Annual Report addresses some of the concerns raised during the consultation by detailing the authorisation process and outlining the IPCO approach to overseeing these powers.

The inspection of public authorities' use of investigatory powers

IPCO subsumed the roles of three previous regimes. These were the Interception of Communications Commissioner's Office; the Intelligence Services Commissioner; and the Office of Surveillance Commissioners.

Apart from UKIC, police and law enforcement bodies, a number of public authorities (such as local councils, trading standards officers and fire & rescue services) have limited powers under the investigatory powers legislation. Even though the powers are seldom used by the latter, IPCO's inspections ensure that these authorities are aware of what the law provides.

The three predecessor bodies listed above published Annual Reports detailing their oversight activities. A consolidated report is now produced by IPCO. In 2019, IPCO published its report on the outcome of its inspections of public authorities for 2017. These reports are a key part of delivering effective oversight and ensuring problems, such as errors, are effectively addressed. Please see the supplementary material for further detail.

The Judicial Commissioners

Fifteen Judicial Commissioners serve in IPCO under the IPC. All Judicial Commissioners are retired senior judges.

The IPC's Deputy is the Rt Hon Sir John Goldring. Sir John was formerly the Intelligence Services Commissioner and Senior Presiding Judge for England & Wales following a career as a High Court Judge of the Queen's Bench Division. Sir John is currently the President of the Court of Appeal in the Cayman Islands and recently acted as Her Majesty's Assistant Coroner for the Hillsborough Inquests.

Parliamentary Oversight

Overview

Parliament plays a critical role in governing the use of investigatory powers:

- At the most fundamental level, it is Parliament **that scrutinises, amends where necessary, and ultimately passes the laws** which provide for the use of these powers. Statutory Codes of Practice under IPA and related legislation such as RIPA are also subject to Parliamentary approval. In addition, the **IPA is subject to review in 2021**.
- The Secretaries of State who issue warrants under IPA, and who are responsible for the activities of UKIC, **are themselves accountable to Parliament**. They may be questioned by Parliamentary committees and by Parliament as a whole at departmental questions.
- Finally, **oversight of the activities of the Agencies themselves is conducted by the Intelligence and Security Committee of Parliament (ISC).** The ISC's role is described below.

Intelligence and Security Committee of Parliament

The ISC was first established by the Intelligence Services Act 1994 to examine the policy, administration and expenditure of the Security Service, SIS, and GCHQ.

The Justice and Security Act 2013 [see supplementary material] reformed the ISC: making it a Committee of Parliament; providing greater powers; and increasing its remit, including

oversight of operational activity and the wider intelligence and security activities of Government. The ISC also has the power to refer matters to the IPC.

The ISC is able to request information and documents from the Agencies in relation to its investigations and inquiries. Information and documents may only be withheld with the express approval of the relevant Secretary of State, and then only for a limited number of specific reasons. In practice, very little is ever withheld from the ISC.

In the course of their investigations and inquiries, the ISC is able to take evidence from all interested parties, including NGOs, other representative bodies and individual members of the public, as well as the Agencies.

Other than UKIC, the ISC examines the intelligence-related work of the Cabinet Office including: the Joint Intelligence Committee (JIC); the Assessments Staff; and the National Security Secretariat. The Committee also provides oversight of Defence Intelligence in the Ministry of Defence and the Office for Security and Counter-Terrorism in the Home Office.

Members of the ISC[45] are appointed by Parliament and the Committee reports directly to Parliament. The Committee may also make reports to the Prime Minister on matters which are national security sensitive.

The Justice and Security Act 2013 requires the Committee to make an Annual Report to Parliament on the discharge of its functions. These reports are first submitted to the Prime Minister who is required to consider, in consultation with the ISC, whether any matters should be excluded in the interests of national security.

In addition to its Annual Reports, the ISC may publish Special Reports. The majority of the Committee's Special Reports, like its Annual Reports, are made to both the Prime Minister (in classified form) and to Parliament (with sensitive material redacted). However, a small number of reports, which deal with the most highly classified matters, may be made solely to the Prime Minister.

Recent reports have included [see supplementary material]:

- **Report on the Draft Investigatory Powers Bill (February 2016).**
  This Report describes the Committee's response to the intelligence agency-related aspects of the Government's draft Investigatory Powers Bill and builds upon the recommendations made in the Committee's Privacy and Security Report of March 2015.

[45] Current members are listed here: http://isc.independent.gov.uk/committee-members

- **Privacy and Security: A modern and transparent legal framework (March 2015)**
  This Report included, for the first time in a single document, a comprehensive review of the full range of intrusive capabilities available to the UK intelligence Agencies. It contains an unprecedented amount of information about those capabilities, the legal framework governing their use, and the privacy protections and safeguards that apply.

  The Report also revealed the use of certain capabilities – such as Bulk Personal Datasets and Directions under the Telecommunications Act 1984 – for the first time. The Report represented a landmark in terms of the openness and transparency surrounding the Agencies' work.

Transparency Reports

The proportionate use of investigatory and disruptive powers is essential to tackle the threats that the UK faces from terrorism and crime. But in a democracy it is right that those powers are only used when it is necessary to do so and that the Government is as transparent as possible about their use. To this end, the Government publishes Transparency Reports on disruptive and investigatory powers.

The 2018 Report explains key investigatory powers and describes the safeguards that apply to their use. The Interception of Communications Commissioner published figures in relation to interception, including the total number of interception warrants authorised, and on the use of communications data by public authorities. These figures are now published by the IPC.

This statistical information is summarised in the Report along with statistics on the use of covert surveillance, covert human intelligence sources and property interference.

The Report also summarises the activities of the Commissioners, including statistical information relating to errors made by law enforcement agencies and UKIC in their use of investigatory powers, and provides information on the casework of the Investigatory Powers Tribunal.

Key figures and statistics from the 2018 report include:

- The **analysis of bulk data has played an important part in every major counter terrorism investigation of the last decade**, including in each of the **22 plots thwarted in the last four years;**
- **Bulk data** enabled **over 90% of the UK's targeted military operations** during the campaign in the south of Afghanistan;
- Bulk data was essential in identifying **95% of the cyber-attacks** on people and businesses in the UK discovered by the agencies in the latter part of 2016;

- **Communications data has played a role in every major Security Service counter-terrorism operation over the past decade** and has been used in 95% of all serious organised crime prosecution cases handled by the Crown Prosecution Service;
- In 2016, 65% of interception warrants were issued for the purpose of the prevention and detection of serious crime presenting no change from 2015; **33% were issued in the interest of national security compared to 34% in 2015**, and 2% were issued in relation to a combination of statutory purposes, up from 1% in 2015; and
- In 2016, **50% of communications data acquired was subscriber data; 48% was traffic data; and 2% was service use data**. The majority of items of data acquired (81%) related to telephony identifiers, such as landline or mobile phone numbers; 15% related to internet identifiers, such as email addresses or IP addresses; 2% related to postal identifiers, such as postal addresses; and the remaining 2% related to "other" identifiers, such as bank account or credit card numbers.

PART V: REDRESS

Overview

The UK has world leading and independent redress mechanisms available to individuals who feel they may have been the subject of unlawful surveillance. In particular, these are provided through the Investigatory Powers Tribunal (IPT); ICO; and Courts and Tribunals.

This part summarises the following key redress mechanisms:

- Redress through the IPT;
- Redress through the ICO;
- Redress through Tribunals if ICO has failed to respond to a complaint;
- Redress through Tribunals in relation to challenging a national security certificate;
- Redress through Courts.

Redress through the IPT[46]

Overview
The Tribunal was established in October 2000 under the Regulation of Investigatory Powers Act (RIPA) 2000. It provides a right of redress for anyone who believes they have been a victim of unlawful action by a public authority improperly using covert investigative techniques.

The Tribunal considers:

- complaints about the use of covert techniques under RIPA, the Investigatory Powers Act 2016, the Intelligence Services Act 1994 and the Police Act Part III against any public authority with powers;
- complaints about any conduct by or on behalf of UKIC;
- Human Rights Act claims about any conduct by or on behalf of the UK Intelligence Community and has exclusive jurisdiction in this regard;
- Human Rights Act claims against the organisations listed in RIPA 65(6) as amended in relation to covert techniques. The Tribunal has exclusive jurisdiction here too.

Members of the Tribunal must be senior members of the legal profession, and the President must have held high judicial office. In practice, the Vice President also holds high judicial office. There are currently ten Members of the Tribunal, including the President The Right Honourable Lord Justice Singh.

[46] This section has relied upon material taken from the Investigatory Powers Tribunal's website www.ipt-uk.com

How the IPT works

The Tribunal is unique in that it:

- can order, receive, and consider evidence in a variety of forms, even if the evidence may be inadmissible in an ordinary court;
- is **free of charge** and the applicant does not have to hire a lawyer. Even if he or she loses the case, the Tribunal has never awarded costs to the public authority being complained about, and it is unlikely it would do so. Generally, the Tribunal will not make an order against a losing party for reimbursement of the costs incurred by the opposing party;
- can **provide confidentiality to protect the claimant** and the fact that he or she has made a complaint. It is concerned not to discourage people from coming forward to make a complaint, who might be apprehensive about possible repercussions;
- can also **protect the identities of other people** if harm is likely to be caused. It has done so, for instance, by giving anonymity to witnesses who would, for good reason, not in other circumstances give evidence;
- can **review material that may not otherwise be searchable and obtain evidence where the applicant acting alone could not**. It is able to do this because it has the power to do so and is required to keep from disclosure sensitive operational material given by UKIC. It therefore has greater freedom to look at this kind of material than the ordinary courts;
- adopts an **inquisitorial process to investigate complaints** in order to ascertain what has happened in a particular case. This is in contrast to the wholly adversarial approach followed in ordinary court proceedings;
- has **wide powers to make remedial orders and awards of compensation**. For instance, it can stop activity, quash authorisations, order material to be destroyed and grant compensation to the extent necessary to give due satisfaction;
- is generally required to keep from disclosure sensitive operational material given by UKIC. The complainant may not be aware of what the Tribunal has seen and will not be entitled to hear or see it, just as, **unless a complainant consents, documents supplied by him or her to the Tribunal will not be disclosed**;

There is a right of appeal from decisions and determinations of the Tribunal on points of law that raise an important point of principle or practice, or where there is some other compelling reason for granting leave to appeal. Where leave to appeal is granted, the appeal will be determined by either the Court of Appeal in England and Wales or the Court of Session in Scotland.

To the extent that a ruling of the Tribunal involves ECHR rights, it is possible to challenge a

decision of the Tribunal by making an application to the European Court of Human Rights in Strasbourg, once all routes to domestic remedy have been exhausted.

Key Facts and Figures about the IPT

- In 2016 the IPT received **209 cases with an additional 297** cases as a result of the Privacy International Campaign, thereby increasing the **yearly total to 506** (IPT Report, 2016).

- In 2016 the **IPT sat on 11 occasions in open court**. Those open inter parties hearings related to 4 complaints. In addition, the Tribunal also sat in **April 2016 to consider 10 complaints as representative of 663 complaints** which were a direct result of the **online Privacy International campaign** (IPT Report, 2016).

- Of the **complaints** received by the IPT in 2016, **35% related to UKIC**, 44% related to law enforcement agencies, 8% related to local authorities and 13% to other public authorities (IPT Report, 2016).

Open Justice

The Tribunal has taken a number of steps to enhance open justice. The Tribunal's policies and procedures have been carefully developed and have evolved with the aim of balancing the principles of open justice for the complainant with a need to protect sensitive material. The approach of hearing a case on the basis of assumed facts has proved to be of great value.

This approach means that, without making any finding on the substance of the complaint, where points of law arise the Tribunal may be prepared to assume for the sake of argument that the facts asserted by the claimant are true; and then, acting upon that assumption, decide whether they would constitute lawful or unlawful conduct.

This has enabled hearings to take place in public with full adversarial argument as to whether the conduct alleged, if it had taken place, would have been lawful and proportionate.

The Tribunal also publishes its significant rulings on its website, providing that this runs no risk of disclosure of any information *"to any extent, or in any manner that is contrary to or prejudicial"* to the national security of the UK.

Counsel to the Tribunal

Over the last 12 years, the Tribunal has developed the practice of instructing its own counsel, known as Counsel to the Tribunal, in certain cases.

Counsel to the Tribunal does not represent any of the parties in a case but nor is he or she a "special advocate" of the kind. The closest analogy is with 'Counsel to a public inquiry'. Counsel to the Tribunal's function is to assist the Tribunal in whatever way the Tribunal directs.

For example, occasionally the Tribunal will not specify from what perspective submissions are to be made. In these circumstances, Counsel will make submissions according to his or her own analysis of the relevant legal or factual issues, seeking to give particular emphasis to points not fully developed by the parties.

At other times, the Tribunal may invite its Counsel to make submissions from a particular perspective: normally the perspective of the party or parties whose interests are not otherwise represented.

The recent judgment of the Strasbourg Court in the *Big Brother Watch* case (nrs. 58170/13, 62322/14 and 24960/15, ECHR 2018) noted, it would appear with approval, the role of Counsel to the Tribunal and how it can help to ensure that the overall procedure is fair.

Significant cases

Since 2013, the Tribunal has heard four very significant cases relating to the Agencies' use of investigatory powers.

The first of these cases was ***Liberty/Privacy*** (IPT/13/77/H IPT13/92/CH IPT/13/168-173/H IPT/13/194/CH IPT/13/204/CH: Reported in [2015] 3 AER 142). In a Judgment dated 5 December 2014 [see supplementary material], and on the basis of assumed facts, the Tribunal considered the lawfulness of the alleged receipt by the Agencies of intercept from two interception programmes operated by the Security Services of the United States, Prism and Upstream, and of the regime of interception by the UK Agencies pursuant to warrants issued under Section 8(4) of RIPA. The Tribunal concluded that the Section 8(4) regime was lawful and Human Rights compliant.

As for Prism and Upstream, the Tribunal concluded that, prior to the proceedings and the judgment of the Tribunal, there had been inadequate disclosure of the regime to be compliant with Article 8 ECHR but that since the disclosures recorded in the Tribunal's judgment it had been compliant, with one possible exception, which was reserved for further argument.

In a Judgment dated 6 February 2015 [see supplementary material], the Tribunal addressed this possible exception and accordingly declared that, prior to the disclosures made and referred to in the earlier judgment and this judgment, the regime governing the soliciting, receiving, storing, and transmitting by UK authorities of private communications of individuals located in the UK which had been obtained by US authorities pursuant to Prism

and/or on the Claimants' case Upstream, contravened Articles 8 or 10, but that the regime now complied with the ECHR.

By an Amended Open Determination dated 22 June 2015 [see supplementary material], the Tribunal made a determination in favour of Amnesty International and the Legal Resources Centre of South Africa that there had been breaches of procedure by GCHQ such as to amount to an infringement of their rights under Article 8 of the Convention but made no order for compensation in their favour.

The second case was ***Privacy International and Greennet & Others*** (IPT 14/85/CH 14/120-126/CH). In their Judgment dated 12 February 2016 [see supplementary material], the Tribunal considered the Claimants' allegations as to the activities of GCHQ in carrying out Computer Network Exploitation (CNE), colloquially 'hacking', pursuant to warrants under Sections 5 and 7 of the Intelligence Services Act 1994.

The Tribunal was asked to consider several issues of law, based on assumed facts, as to whether such activity was or would be lawful in accordance with domestic law and Articles 8 and 10 of the ECHR.

The Tribunal concluded that acts of CNE pursuant to such warrants by GCHQ would in principle be lawful both before and after the amendment of Section 10 of the Computer Misuse Act 1990 in 2014. The Tribunal considered and gave guidance as to how specific a Section 5 warrant would have to be in its description of the property in respect of CNE and concluded that warrants compliant with such guidance would be lawful both at domestic law and so comply with the Convention.

The Tribunal considered the Covert Surveillance Property Interference Code (as amended from time to time since 2002) and the draft 2015 Equipment Interference Code of Practice, which in practice had been in effect since February 2015, and concluded that the regime governing the operation of Section 5 warrants, both before and after February 2015, complied with Articles 8 and 10 of the ECHR.

In relation to a Section 7 warrant concerning the authorisation of acts outside the British Islands, there was an issue as to whether the Convention would apply, at least in the absence of particular facts relating to an individual case, and the Tribunal therefore reached no conclusion that the Section 7 regime was non-compliant with the Convention.

In relation to the specific issue of the adequacy of dealing with legal and professional privilege, the Tribunal concluded that the CNE regime had been compliant with the Convention since February 2015.

The third case was ***Privacy International*** (IPT/15/110/CH). This case concerned the acquisition and use by the UKIC of:

- Bulk Personal Datasets (BPD); and
- Bulk Communications Data (BCD).

UKIC have used statutory powers to obtain BPD including data relating to large numbers of individuals, most of whom are unlikely to be of any intelligence interest (including data from telephone directories, passport databases and commercial databases) but which are of great utility by way of electronic search for information that can be of use for counter-intelligence or the detection of crime.

This was revealed by the Intelligence and Security Committee of Parliament in March 2015. In addition, it was revealed in November 2015 that Secretaries of State had been using the power to issue directions to communications providers under Section 94 of the Telecommunications Act 1984 in order to obtain and retain large quantities of communications data (BCD) for similar purposes in the interest of national security.

The Claimant (Privacy International) contended that this obtaining and use of BCD pursuant to Section 94 is unlawful at English domestic law and contravenes both the ECHR and EU law, and that the obtaining/use of BPD is contrary to the ECHR and EU law.

In a Judgment dated 17 October 2016 [see supplementary material], the Tribunal held:

1. That the obtaining of BCD pursuant to section 94 was not unlawful at domestic law, and antedated the statutory scheme under Chapter II of Part I of RIPA 2000 and was not repealed by it, but was in any event preserved by the Communications Act 2003.

2. That neither the obtaining of BPD nor of BCD complied with Article 8 of the ECHR prior to their avowal in March/November 2015, by virtue of their lack of foreseeability to the public and in relation to BCD, the lack of adequate oversight by the independent Commissioners.

3. That following avowal of the position and publication of the relevant procedures, and changes to the oversight arrangements, the powers were, since March/November 2015 respectively, compatible with Article 8.

The Tribunal invited further submissions and adjourned to a later date consideration of:

- The issue as to EU law;
- Consideration of the issue of proportionality; and
- Transfer of data to third parties.

In a subsequent Judgment dated 8 September 2017 [see supplementary material], the Tribunal said: "In our judgment, it is unclear whether, having regard to Article 4 TEU, and Article 1(3) EPD [the ePrivacy Directive (2002/58/EC)], the activities of the security and intelligence agencies in relation to the acquisition and use of BCD for the purposes of national security:

- are to any extent governed by Union law;

- are subject to the requirements of Article 15(3) EPD in accordance with the decision in Watson [(C-698/15, ECLI:EU:C:2016:970)], or, in accordance with Article 4 TEU [Treaty on European Union] and Article 1(3) EPD, and following the decisions in Parliament v Council and Ireland v Parliament, should be treated as outside the scope of the EPD; or

- are subject to the requirements stipulated by the decision in Watson at paragraphs 119 - 125 and, if so, to what extent, taking into account the essential necessity of the UK Intelligence Community to use bulk acquisition and automated processing techniques to protect national security and the extent to which such capabilities, if otherwise compliant with the ECHR, may be critically impeded by the imposition of "such requirements".

In a Judgment dated 30 October 2017 [see supplementary material], the Tribunal therefore made a request to the Court of Justice of the European Union for a preliminary ruling pursuant to Article 267 TFEU in relation to BCD. This case is currently before the CJEU (C-623/17).

In a final Judgment dated 23 July 2018 [see supplementary material], the Tribunal, dealing with the matters outstanding from its Judgments of 17 October 2016 ([2017] 3 AER 647) and 11 September 2017 ([2018] 2 AER 166) relating to Bulk Communications Data (BCD) and Bulk Personal Data (BPD) concluded unanimously (save in relation to one issue, set out below):

1. That in relation to many directions made prior to October 2016 by the Foreign Secretary to Communications Service Providers to provide BCD to GCHQ, they were not in accordance with law.

2. (By a majority) that the regime in respect of sharing of BCD/BPD with foreign agencies complies with Article 8 of the ECHR.

3. That the regime in respect of sharing BCD/BPD with industry partners complies with Article 8 ECHR.

4. That the steps taken by way of collection, retention and use of BCD or BPD by the Respondents comply with the requirements of proportionality pursuant to Article 8 ECHR and EU law.

The Tribunal further unanimously dismissed an application by the Claimant to set aside its conclusions in its Judgment of 17 October 2016.

The Tribunal delivered a Closed Judgment, with conclusions that were consistent with those in its Open Judgment.

In September 2018, the Tribunal made a determination in favour of the Claimant, pursuant to section 68(4) of RIPA. This determination relates only to the Human Rights Act 1998 complaint that has been made by the Claimant. The Tribunal is awaiting the ruling of the CJEU on the preliminary reference before it can make a determination in relation to the complaint that the use of section 94 of the Telecommunications Act 1984 was contrary to EU law. The Tribunal has yet to hand down their reasonings for the September 2018 determination after which it will invite submissions on remedies.

The fourth significant case was a challenge brought forward in July 2017 against a large part of the IPA by ***Liberty (CO/1052/2017)*** which received its most recent judgement from the High Court in July 2019.

The Court initially granted permission for the Claimants to proceed only with the elements of the claim relating to Part 4 (retention of CD) with the remainder of the claim stayed as those provisions were not yet in force. Some elements of the Part 4 claim were also stayed pending a further reference from the Investigatory Powers Tribunal (IPT) to the European Court of Justice (ECJ). That case remains pending and will be considered once the ECJ case concludes.

The judgement for this part of the claim was handed down in April 2018 for which the **Court found in favour of the Government** save for two areas which the UK Government conceded on. First, the acquisition of communications data should be subject to prior independent review and, second, when acquiring more intrusive data for crime purposes, there should be a serious crime restriction. In October 2018, the Government amended the IPA to remedy these defects.

In 2018, the Claimants were given permission to proceed with the remainder of their claim which related to four different sets of provisions in the IPA, all concerning the Act's provision for bulk powers. On this, Liberty specifically claimed that:

a. The provisions in the IPA under challenge are incompatible with Article 8 (the right to respect for private life and correspondence) and Article 10 (the right to freedom of expression) of the ECHR because they are too wide. Liberty also claimed that they lack the "minimum safeguards" established by the ECHR for secret surveillance regimes and that they are neither necessary in a democratic society nor proportionate.

b. The powers lack sufficient safeguards to comply with the "min. requirements" taken together. For this reason they are said not to be "in accordance with the law" (the phrase used in Article 8) or "prescribed by law" (that used in Article 10).

c. The powers lack sufficient safeguards for lawyer-client communications and journalistic material, including the confidential sources of a journalist's information.

d. The continued operation of Part 1, Chapter 2, RIPA, which concerns the acquisition of communications data, is not in accordance with law because it does not comply with EU law. They claimed that although amendments were made to Parts 3 and 4 of the IPA in accordance with the declaration granted by the High Court, the previous regime had not been repealed.

In the High Court Judgement dated 29 July 2019 [see supplementary material]**, the Court found in favour of the UK Government on all counts and refused the Claimant's request for a declaration of incompatibility under section 4 of the Human Rights Act 1998**. In particular, the Court concluded that:

1. **It did not accept** the Claimant's suggestion that the purposes for which **Parts 3 and 4 of the IPA** may be exercised are **too wide or arbitrary**. It stated that:

   "The mere fact that under Part 3, powers may be obtained by a range of public authorities does not support an argument of incompatibility. The key consideration is what are the relevant powers, procedures and safeguards, and how are they defined. We have not seen anything in the material put before us to indicate that Parliament has enacted legislation giving rise to the risk of arbitrary interference or any other incompatibility with the Convention rights."

2. It was **not persuaded that the IPA is incompatible with ECHR** insofar as the challenge concerns the bulk interception powers regime. In this, the Court noted the **important reality that the ability to effect interception in bulk is a critical capability for the intelligence services in so far as to protect the public** and set out the importance of the **double lock** safeguard and role of the IPC that the IPA introduced. On the IPC, the Court stated that it was important for the Claimant not to overlook the powers given to the IPC, in particular under section 229 of the Act, to oversee the whole interception process. It stated that:

"Ultimately, sight must also not be lost of the fact that it is open to a person to make a complaint or bring a claim under the HRA to the IPT. The question, therefore, of whether there has been a breach of the HRA on the facts of a particular case is something that can in principle be raised and adjudicated by an independent tribunal which can have access to all relevant material, including secret material. This is another feature of the statutory scheme which persuades us that it is not the 2016 Act itself which can be said in the abstract to be incompatible with the Convention rights."

3. It accepted that the **safeguards applicable to CD examination**, including the absence of a British Islands safeguard, **provide adequate protection against arbitrary interference** with rights under Articles 8 and 10 of ECHR. In particular it stated that:

"We see no basis for this Court to conclude that Chapter 2 of Part 6 is not in accordance with the law and therefore incompatible with Articles 8 or 10 of the ECHR."

"In our judgement the legal framework applicable to bulk acquisition of CD provides sufficient independent oversight of selectors and search criteria, so as to overcome the criticism made of the regime governing section 8(4) of RIPA in Big Brother Watch, at para. 340."

4. The scope of application of the bulk equipment interference power **is not too wide to be incompatible with Articles 8 and 10 of the ECHR** and that both the IPA and Equipment Interference Code of Practice contains sufficient provisions as to the need for specificity of warrants. It stated that:

"In the present context Parliament has created a scheme for the grant of warrants in prescribed circumstances which are carefully regulated by the 2016 Act and the codes of practice made under it as well as the supervision of the office of the IPC."

5. It **did not accept** the Claimant's argument that **Bulk Personal Datasets** (BPDs) powers conferred by Part 7 are **too wide to be compatible** with Articles 8 and 10. It also **acknowledged the importance** of BPDs, stating:

"BPDs enable targets to be identified and swift action to be taken to counter a threat. The obtaining of accurate information at great speed has a considerable value. Many alternatives would be slower, less comprehensive or more intrusive. In some areas, particularly pattern analysis and anomaly detection, no practicable alternative to the use of BPDs exists."

6. The **safeguards in the IPA in relation to lawyer-client communications are sufficient** to comply with Article 8 of the ECHR. It was satisfied that the rules regarding legally

privileged items are set out in the Act and Codes of Practice with sufficient clarify and with sufficient safeguards to prevent arbitrary interference.

7. The court is satisfied that the rules regarding legally privileged items are set out in the Act and Codes of Practice with sufficient clarity and with sufficient safeguards to prevent arbitrary interference. The Court concludes the **scheme is therefore compatible with Article 8.**

8. The safeguards in relation to journalistic material **ensure compliance with Article 10 of the ECHR**.

Redress through the ICO

The ICO's powers and responsibilities are set out in detail in Section G of this pack.

The national security exemption mentioned earlier also specifies provisions within Part 5 (the Information Commissioner) and Part 6 (Enforcement) of the DPA 2018 that can be exempt for the purposes of safeguarding national security.

The ICO has general powers to receive complaints and take enforcement action in respect of any matters of concern relating to the rights of data subjects. In some circumstances, these regulatory powers can be disapplied where the exercise of those powers would interfere with the purposes of safeguarding national security.

The approach taken in respect of the national security exemption is consistent with the approach taken previously in the DPA 1998 and ensures that data controllers are held to a high standard of protection of personal data.

The ICO is required to publish a record of each national security certificate. This ensures that individuals who believe they are directly affected by a certificate are better able to exercise their rights.

If individuals believe that the high standards of protection provided for in Part 4 of the DPA 2018 have not been met, or they have another complaint not covered by the jurisdiction of the IPT, **they can make a complaint to the ICO**.

Redress through Tribunals if the ICO has failed to respond to a complaint

If the ICO fail to take appropriate steps in relation to a complaint or fails to respond within three months, the individual **may apply to the First-Tier Tribunal and, ultimately, appeal to the Upper Tribunal** (in the General Regulatory Chamber). The Tribunals can make an order

compelling the Commissioner to respond to a complaint raised by a data subject under the UK GDPR where it determines that she has failed to do so.

In other circumstances individuals alleging a breach of the DPA 2018 can consider taking a challenge to the High Court (or Court of Session in Scotland).

Redress through Tribunals in relation to challenging National Security Certificates

Any person directly affected by a national security certificate may challenge the certificate in the Upper Tribunal. The Tribunal Procedure (Upper Tribunal) Rules 2008, as amended by the DPA 2018, set out the process and procedure for such appeals.

When considering such a challenge, the Tribunal applies the principles applied by a court on an application for judicial review. In applying such principles, the Upper Tribunal can consider a wide range of issues, including necessity, proportionality and lawfulness.

This would enable, for example, the Upper Tribunal to consider whether the decision to issue the certificate was reasonable, having regard to the impact on the rights of data subjects and balancing the need to safeguard national security. If they conclude that the Minister did not have reasonable grounds for issuing the certificate, the Tribunal can allow the appeal and quash the certificate.

The ability to challenge a national security certificate is not purely academic. It offers the ability to independently scrutinise decisions to issue certificates and challenge the basis on which they were issued and the scope of certificates.

For example, the first certificate issued to MI5 under section 28(2) of the DPA 1998 was quashed following a legal challenge (the Norman Baker case in 2001), with the then Data Protection Tribunal finding that the certificate was wider than necessary to protect national security. The Tribunal also recognised that there were occasions where data could be released to individuals without prejudicing national security.

This decision demonstrates that this mechanism is an important means of ensuring transparency and accountability.

Individuals may also appeal to the Upper Tribunal to challenge the application to specific personal data of a national security certificate that identifies the restriction to which it applies by means of a general description.

Redress through courts

Section H: National Security Data Protection and Investigatory Powers Framework

Alongside the ICO, the DPA 2018 provides the courts (as distinct from the Tribunals) as another mechanism of redress. The DPA 2018 provides the courts with a number of powers, including:

- the granting of a search warrant to the Commissioner where the Court is satisfied that an offence has been committed by the named controller and that evidence of the offence is found on the premises;

- the making of an order requiring a controller to take, or refrain from taking particular steps where the court considers that there has been an infringement of a data subject's rights;

- ordering a controller to comply with an Information Notice;

- ordering compensation where a data subject has suffered damage because of a contravention of the law.