Department for
Science, Innovation
& Technology

Paper prepared by the UK Government in support of our designation as a qualifying state under US Executive Order 14086

September 2023

Any enquiries regarding this publication should be sent to us at:
alt.formats@dsit.gov.uk.

Contents

Foreword

International data transfers drive international commerce, trade and development, support international cooperation and underpin law enforcement and national security. The UK Government is committed to reducing barriers to data flows in order to unlock growth and make it easier for UK businesses to trade, whilst ensuring that high data protection standards are maintained and individuals' data is robustly protected.

Building on the strong bilateral UK-US relationship, a UK-US data bridge was outlined as a priority for 2023 at the inaugural UK-US Comprehensive Dialogue on Data and Technology, representing a key milestone in both countries' commitment to ensuring the free and trustworthy flow of data[1].

Both the UK and US are committed to high standards of data protection and trust being at the forefront of the data bridge. A vital element of these protections is the existence of effective redress and routes to rectify any unlawful interference with personal data.

The UK's regulation of investigatory powers has had these principles at its core for many years, as reflected most recently in the Investigatory Powers Act 2016 (IPA). The independent oversight mechanism provided by the Investigatory Powers Commissioner (IPC) has been acknowledged to be at the forefront of intelligence oversight across the globe and the "double lock", which requires warrants issued under the IPA to be approved both by a Secretary of State and a Judicial Commissioner, ensures that the most intrusive powers require independent prior judicial authorisation for their use.

For over 20 years, the Investigatory Powers Tribunal (IPT) has provided a right of redress for those who believe they have been a victim of unlawful action by a public authority improperly using covert investigative techniques. This highly specialised Tribunal is free of charge – ensuring there is no barrier to redress – and can review material that would likely be inaccessible in normal courts.

The Executive Order 14086 "Enhancing Safeguards for United States Signals Intelligence Activities" (EO 14086)[2] was signed by the President of the United States in October 2022. It sets out a framework for the Attorney General of the United States to designate countries as "qualifying states" which allows individuals in those designated states access to the redress mechanisms established under the Executive Order.

Section 3(f)(i)(A) of the Executive Order requires that, in order to designate the United Kingdom, the US Attorney General must, among other criteria, determine that the laws of the United Kingdom "require appropriate safeguards in the conduct of signals intelligence activities

[1] https://www.gov.uk/government/news/inaugural-meeting-of-us-uk-comprehensive-dialogue-on-technology-and-data.
[2] https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities.

for United States persons' personal information that is transferred from the United States to the territory of" the United Kingdom.

This document is the evidence submitted by the UK Government to the US Attorney General to support designation as a qualifying state under EO 14086. It explains how the UK Intelligence Community (UKIC) could access the personal information of a US person that has been transferred from the US to the UK. The document details the relevant powers that could be used in the collection of data that has been transferred to and is within the UK as well as the applicable safeguards, oversight and redress mechanisms.

UKIC plays a critical role in ensuring the safety and security not just of those living in the UK but of the citizens of our partners and allies as well. Access to data is a vital part of how they are able to protect national security and prevent and detect serious crime. However, at all times their access to data through the use of the investigatory powers must be necessary and proportionate and in line with their statutory purposes, which can be summarised as protecting national security and the economic well-being of the UK and supporting in the prevention and detection of serious crime.

In terms of access to US persons' data, if a US persons' data has been transferred from the US to an entity in the UK, the UK government may compel that UK entity to disclose that US person's personal data for intelligence purposes if it falls within the statutory functions of the intelligence community and where a relevant power under the IPA can be engaged.

The UK and the US both have a long history of legislation in this space, as well as being leaders in pushing for common standards for ensuring legitimate access to data by governments on a global scale. Both countries acknowledge that while the fundamental importance of government access to data in keeping citizens safe cannot be overplayed, it should not come at a disproportionate cost to the privacy of those citizens.

The core principles that both governments hold have been excellently summarised in the recently signed OECD Declaration on Government Access to Personal Data Held by Private Sector Entities[3], as follows:

- A legal basis setting out purposes, conditions, limitations and safeguards concerning government access;
- Legitimate aims for government access. It should not be used to suppress dissent or target groups solely of the basis of certain characteristics;
- There should be prior approval requirements;
- Personal data acquired through government access can only be processed and handled by authorised personnel;
- The legal framework for government access is clear and transparent;
- There is effective and impartial oversight to ensure that government access complies with the legal framework;

[3] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487.

- The legal framework provides individuals with effective judicial and non-judicial redress to identify and remedy violations of the national legal framework.

These are not new principles, but rather ones that are continually being crystalised and codified by the international community. They are principles that, while strengthened over the years, have long been applied in the UK. How these principles are applied in the UK is explained further in this document.

Introduction

The relevant activities of the UK intelligence community (MI5, SIS and GCHQ, collectively "UKIC") are governed principally by three pieces of legislation. Two of these – the Security Service Act 1989 and the Intelligence Services Act 1994 – provide the statutory footing for them to operate and lay out their functions. While there is some small variation between the three organisations, their collective purpose can be summarised as protecting national security and the economic well-being of the UK and supporting in the prevention and detection of serious crime.

The third, and for the purposes of this document, more important piece of legislation is the IPA. As well as providing the statutory basis for the use of investigatory powers, the IPA and its Codes of Practice, provide the safeguards for their use as well as the statutory basis for the Investigatory Powers Commissioner, who is the independent overseer of their use. UKIC also relies on powers in the Regulation of Investigatory Powers Act 2000 (RIPA) to which the IPA is, in part, a successor. However, the powers in RIPA are not relevant for present purposes[4].

Investigatory Powers Act 2016

The IPA brought together many of the UK's existing investigatory powers in one single piece of legislation. The IPA also created the 'double lock' – the requirement for IPA warrants to be approved both by a Secretary of State, or in certain circumstances a Scottish Minister, and then by a Judicial Commissioner. Alongside the requirement for necessary and proportionate use of the powers, the independent oversight by the Investigatory Powers Commissioner, is one of the key cornerstones of the regime.

The Act incorporated the findings of comprehensive reviews undertaken by Lord Anderson KC (formerly the Independent Reviewer of Terrorism Legislation)[5], by the Intelligence and Security Committee (ISC) of Parliament[6] and by a panel convened by the Royal United Services Institute (RUSI)[7]. Collectively, they made 198 recommendations. All three reviews agreed that the use of these relevant powers remained vital.

The IPA puts on a statutory footing the following powers:

- Targeted interception (Part 2);[8]

[4] Part II RIPA sets out powers in respect of directed and intrusive covert surveillance (e.g. mobile surveillance or the use of listening devices) and the conduct and use of Covert Human Intelligence Sources (agents and undercover officers).

[5] A question of trust: report of the investigatory powers review - GOV.UK (www.gov.uk).

[6] HC 795 Intelligence and Security Committee of Parliament – Report on the draft Investigatory Powers Bill (independent.gov.uk).

[7] Independent Surveillance Review Publishes Report: 'A Democratic Licence to Operate' | Royal United Services Institute (rusi.org).

[8] Targeted interception has long been carried out under warrant but that requirement was put on a statutory footing in the Interception of Communications Act 1985 and then again, in a revised form, in Part I of RIPA.

- Targeted communications data (Parts 3 and 4);[9]
- Targeted equipment interference (Part 5);
- Bulk interception, acquisition of communications data and equipment interference (Part 6);
- Retention and examination of bulk personal datasets (Part 7).

Each investigatory power has a corresponding statutory Code of Practice, the purpose and status of which is explained under the relevant heading below.

The safeguards provided for in the IPA reflect the UK's international reputation for protecting human rights, including the right to respect for private and family life in Article 8 of the European Convention of Human Rights (ECHR).[10] Article 8 requires that the interference must be "foreseeable" – that is, have a clear, accessible basis in law – and that the law must contain appropriate safeguards (including 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 restrictions based on the classification of data, firewalling of internal IT, and access restrictions based on the established principle of 'need to know'.

For example, GCHQ has a centralised legal policy and compliance function responsible for ensuring that GCHQ complies with all legal obligations in the course of its operations, including the Investigatory Powers Act. Compliance officers are also embedded within mission and technical teams.

All GCHQ staff and contractors must complete mandatory mission legalities training. Operational staff such as intelligence analysts and mission leads must complete further advanced training modules focused on the legal requirements specific to their role within the organisation. Technical controls prevent staff from requesting or accessing operational data unless they have completed the necessary training. All training must be recertified at regular intervals. Compliance with these training requirements is monitored by GCHQ's central compliance function.

Targeted interception

Targeted interception warrants are an investigative tool that enable the interception of communications, including the content, 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. Interception under targeted

[9] Powers in respect of communications data were previously set out in and under the Telecommunications Act 1984.

[10] The European Court of Human Rights publishes guides to the various Articles of the Convention; the Article 8 case law guides provides an excellent section on the Article 8 jurisprudence on secret surveillance: https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf.

warrants can take place while a communication is in the course of its transmission (e.g. between two devices), or when it is stored before or after transmission.

Warrants can be modified in two ways[11], through either a major or a minor modification:

- Major modifications relate to the adding or varying a name or description of a person, or group of persons, or organisation or set of premises to which the warrant relates. Major modifications can only be made by either the Secretary of State (or Scottish Ministers) or a senior official acting on their behalf.
- Minor modifications relate to the adding, varying or removing of a factor specified in the warrant, for example a target phone number. Additionally, the removal of a name or description of a person, or groups of persons. Minor modifications, in addition to those specified above, can also be made by the person to whom the warrant is addressed, or a person holding a senior position within that public authority.

In the case of 'thematic' warrants that target more than one person (or a group of persons), the target of the warrant could be specified in one of two ways which will have an impact on what type of modification is required to modify them. For example, a warrant could target a number of individually named people; to add new people, a major modification would be required, but to change a factor for one of the existing people, only a minor modification would be required.

A warrant of this kind could also target a group, such as an organised crime group and the name of this group would be target. If a public authority intends to add a factor to this warrant which is attributable to Joe Bloggs/John Doe, they can do this by way of minor modification if it falls into the target of 'organised crime group X'. They do not need to add John Doe by way of major modification, although they could do that if they wish.

The extra safeguards[12] in respect of the communications of members of relevant legislatures, legal professional privilege and journalistic material and sources also apply to major modifications. If these sections are engaged, then the major modification must be approved a Judicial Commissioner[13]. In all other cases, the Investigatory Powers Commissioner's Office (IPCO) must be notified of major modifications that are made[14].

Each of the investigatory powers has slightly different user communities. The intercept community is the smallest. There are only nine public authorities able to apply for the targeted interception powers. They are:[15]

- The Security Service (MI5);
- The Secret Intelligence Service (SIS);
- Government Communications Headquarters (GCHQ);
- The National Crime Agency;

[11] Section 34, IPA.
[12] Sections 26, 27, 28 and 29 IPA.
[13] Section 36(6) IPA.
[14] Section 37, IPA.
[15] Section 18, IPA.

- The Metropolitan Police Service;
- The Police Service of Northern Ireland;
- The Police Service of Scotland;
- His Majesty's Revenue and Customs; and
- The Ministry of Defence.

These intercepting authorities can only conduct targeted interception if they have obtained an appropriate warrant authorised under Part 2 of the Act. Warrants can be issued only when necessary for the statutory purposes of preventing or detecting serious crime, in the interest of national security, or in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security, and when the conduct authorised by the warrant is proportionate to what it seeks to achieve.[16]

All warrants must be issued by the Secretary of State (or Scottish Ministers) 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[17].

The IPA makes it a criminal offence[18] to conduct interception in the UK without lawful authority and stipulates what constitutes lawful authority[19] to do so. This includes when a targeted interception warrant has been issued, subject to the conditions in the IPA.

As with all the investigatory powers, targeted interception has safeguards that include requiring intercepted material to be disclosed only as is necessary and stored safely; and that it may only be held for as long as there are relevant grounds for retaining it[20].

Further strong safeguards are also laid out in the IPA that apply to warrant applications relating to members of Parliament, items subject to legal privilege, confidential journalistic material and sources of journalistic information[21].

There are restrictions on the use or disclosure of material obtained under interception warrants, this includes an offence for making unauthorised disclosures[22]. It should be noted that under the IPA, unlike in the US, interception material cannot be disclosed in any legal proceedings, subject to some exceptions[23].

[16] Section 20 IPA. Necessity and proportionality are explained further in the Interception Code of Practice, paragraphs 4.10 – 4.16.
[17] Sections 19, 21 and 23, IPA.
[18] Section 3, IPA.
[19] Section 6 IPA.
[20] Section 53, IPA.
[21] Sections 26, 27, 28, 29 and 55, IPA.
[22] Sections 57 and 59, IPA.
[23] Section 56 and Schedule 3, IPA.

There are safeguards for the disclosure of intercept material overseas[24]. These specify that requirements corresponding to the requirements of section 53(2) and (5) will apply,[25] to such extent (if any) as the issuing authority considers appropriate, in relation to any of the material which is handed over, or any copy of which is given, to the authorities in question.

Additionally, there should be restrictions in force which would prevent, to such extent (if any) as the issuing authority considers appropriate, the doing of anything in, for the purposes of or in connection with any proceedings outside the United Kingdom which would result in a prohibited disclosure, which means, a disclosure that, if made in the United Kingdom, would breach the prohibition in section 56(1).

Targeted Communications Data

Over 600 public authorities[26] in the UK, including UKIC, can seek a targeted communications data authorisation.

Communications data (CD) refers to the who, where, when, how and with whom of a communication and is often generated by telecommunications and postal operators in the course of their business practices.

Communications data is either entity data or events data[27]. Entity data is data about an entity (e.g. a person's name and address used to register with the telecommunications service). Events data is any data which identifies or describes an event (e.g. the time a message was sent). When a public authority wishes to acquire events data (the more intrusive communications data) for the prevention or investigation of crime, it may only do so if it meets the serious crime threshold that would attract at least a one-year sentence[28].

The acquisition of targeted communications data must be for at least one of the operational purposes listed under the IPA. These are:[29]

- 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;

[24] Section 54 IPA.

[25] The requirements to keep to a minimum necessary the number of people who can access the material, the number of copies made of it, the extent to which it is disclosed and copied and that it is deleted when it is no longer necessary to retain.

[26] Schedule 4, IPA.

[27] Section 261(3) – (5) and (7) IPA.

[28] Section 60A(7) and (8) and section 86(2A), IPA.

[29] Section 60A IPA.

- 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 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.

Under Part 3, public authorities and law enforcement agencies are obliged to make applications for CD to an independent authorising body called the Office for Communications Authorisations (OCDA). The IPC, supported by IPCO, provides oversight of OCDA and of the wider IPA regime. OCDA considers almost all of these CD acquisitions, although for urgent circumstances and for non-serious crime authorisations, the public authorities in question are able to self-authorise.

This independent evaluation and authorisation of each CD application ensures the necessity and proportionality test of each CD request is met[30] and helps to protect the privacy of individuals by providing greater independent oversight. The IPA regime also places the relevant organisations under a legal obligation to provide CD to the public authorities who have had their request for CD authorised by OCDA[31].

To enhance the effective and lawful operation of the powers, in addition to the independent authorisation and inspection regime, the acquisition process is managed by a group of accredited and trained staff called CD Single Point of Contacts (SPoCs).

From 1 January 2023[32], UKIC do not have the power to internally authorise the acquisition of targeted communications data for purposes which relate solely to serious crime, other than in urgent circumstances. This change has been made to implement the Divisional Court findings in the case of R (Liberty) v Secretary of State for the Home Department[33].

UKIC will seek independent authorisations for acquisitions of this type from OCDA. However, these changes to Schedule 4 of the IPA still permit UKIC to acquire CD in urgent circumstances through the internal authorisation process, which requires a member of the senior civil service or above within the requesting organisation to provide that urgent written or verbal authorisation.

OCDA operate during 'normal' office hours only[34] and UKIC need to be able to access targeted communications data at all hours in urgent situations. Therefore, UKIC retain the power to self-authorise the acquisition of targeted communications data for urgent applications where those authorisations relate solely to serious crime.

[30] Part 3, Section 60A, IPA.
[31] Section 66 IPA.
[32] SI/2022/1395, which amends Schedule 4 IPA - https://www.legislation.gov.uk/uksi/2022/1395/made.
[33] [2022] EWHC 1630 (Admin); https://www.bailii.org/ew/cases/EWHC/Admin/2022/1630.html.
[34] https://www.ipco.org.uk/ocda/.

It should be noted that law enforcement bodies such as police forces are already able to self-authorise urgent targeted communications data requests in the same way. Implementing the Court's judgment simply puts UKIC in the same position as the police in relation to serious crime applications.

Data protection law requires telecommunications and postal operators to delete data that they no longer require for business purposes. It is therefore necessary to have a power to require operators to retain specified data in certain circumstances, given its importance to investigations - where it is necessary and proportionate to do so.

The IPA provides for the acquisition and retention of communications data in Parts 3 and 4 respectively. Part 4 provides that the Secretary of State may, by notice, require telecommunications and postal operators to retain communications data for up to 12 months, subject to strict limitations and safeguards. The notice does not require them to retain the content of the communication. The existence and contents of a retention notice must not be disclosed and all notices have to go through the double lock process as well as being annually reviewed to ensure they still meet the necessity and proportionality requirements.

Chapter 13 of the Communications Data Code of Practice lays out the general safeguards for communications data. These include that communications data obtained as a consequence of an interception warrant must be treated in accordance with the safeguards in section 53[35]. That all copies, extracts and summaries of communications data must be held to an adequate level of protection for the relative sensitivity of the data and meets the relevant data protection principles[36]. The data must also be protected against unauthorised access[37] and accessed only by trained individuals, the number of whom should be kept to the minimum necessary[38].

The Code also states that communications data may only be held for as long as the relevant public authority is satisfied that it is still necessary for a statutory purpose and that once it is no longer necessary or proportionate to hold the data, all copies must be destroyed[39]. Additionally, the Code specifies the safeguards for the disclosure of communications data to overseas authorities[40].

Targeted Equipment Interference

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[41].

[35] Paragraph 13.5, Communications Data Code of Practice.
[36] Paragraph 13.6, Communications Data Code of Practice.
[37] Paragraph 13.6, Communications Data Code of Practice.
[38] Paragraph 13.7, Communications Data Code of Practice.
[39] Paragraph 13.10, Communications Data Code of Practice.
[40] Paragraphs 13.32 - 13.36, Communications Data Code of Practice.
[41] Section 100, IPA.

Like all investigatory powers, the use of targeted equipment interference must meet the test of necessity and proportionality and must be necessary in the interests of national security, for the prevention and detection of serious crime, or in the interests of the economic well-being of the UK insofar as those interests are relevant to the interests of national security[42].

As with targeted interception warrants, targeted equipment interference warrants must be double locked[43], it is also possible to have a thematic equipment interference warrant[44]. The same safeguards as for interception on retention, review and deletion of data also apply to equipment interference[45]. Targeted equipment interference warrants are valid for up to six months[46] (except urgent warrants which are only valid for three working days[47]).

Like with targeted interception, there are 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[48]. There are also safeguards for dissemination of the material overseas[49].

Bulk Communications Data

Bulk communications data (Part 6, Chapter 2) may only be sought by UKIC and refers to the acquisition of communications data in bulk from a telecommunications operator.

Bulk communications data (BCD) can only be acquired where it is necessary and proportionate to do so, as with other powers. At least one of the grounds for issuing a bulk communications data warrant must always be that the warrant is necessary in the interests of national security[50]. Each warrant must be clearly justified and balance intrusions into privacy against the expected intelligence benefits. Bulk communications data warrants, like all warrants, require a double lock by a Judicial Commissioner[51].

Bulk communications data warrants must also specify the more detailed operational purposes for which material acquired under those warrants may be examined.[52] An operational purpose may not be specified on an individual bulk communications data warrant unless it is a purpose that is specified on the central list maintained by the UKIC agency heads[53].

---

[42] Section 102, IPA.
[43] Section 108 IPA.
[44] Section 101,IPA.
[45] Section 129, IPA.
[46] Section 116, IPA.
[47] Section 109, IPA.
[48] Sections 111, 112, 113, 114 and 131, IPA.
[49] Section 130, IPA.
[50] Section 158, IPA.
[51] Section 159, IPA.
[52] Section 161(3) IPA.
[53] See section 263 IPA: the Director General of the Security Service (MI5); the Chief of the Secret Intelligence Service (MI6); the Director of GCHQ.

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 of Parliament[54].

Selection for examination of any data acquired and retained under a bulk communications data warrant must always be necessary and proportionate for at least one of the operational purposes specified on the warrant[55]. There are also safeguards for deletion, retention and overseas dissemination[56].

Bulk communications data allows UKIC to conduct far more complex analysis of all relevant data at speed where discovery through individual requests would be significantly slower. Analysis of BCD include identifying (and ruling out) links to known targets, patterns of behaviour, activities of interest, travel patterns and the links between known associates or plotters. UKIC can then take the necessary action to stop attacks e.g., when analysis of the BCD alerts them to changes in behaviour that might indicate an imminent terrorist attack.

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[57]. 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[58].

Bulk Equipment Interference and Bulk Interception

Bulk interception warrants authorise the interception of overseas-related communications and the subsequent selection for examination of the intercepted material[59]. Interception under bulk warrants can take place while a communication is in the course of its transmission (e.g. between two devices), or when it is stored before or after transmission. Bulk interception is an intelligence gathering tool that is used, for example, to identify previously unknown threats to the national security of the UK. Bulk equipment interference warrants authorise the acquisition of overseas-related communications, equipment data and information described in the warrant and/or the selection for examination of such material[60].

The safeguards set out in the section relating to bulk communications data regarding the double lock, operational purposes, retention, disclosure, selection for examination, maintenance of examination records with associated necessity and proportionality

[54] Section 161(6) – (10), IPA.
[55] Section 172, IPA.
[56] Section 171, IPA.
[57] Paragraphs 6.15 and 6.16, Bulk Acquisition of Communications Data Code of Practice.
[58] Section 173, IPA.
[59] Section 136, IPA.
[60] Section 176, IPA.

justifications, and the criminal offence for deliberate breach of IPA safeguards also apply to bulk interception and bulk equipment interference[61].

The IPA also provides additional safeguards relating to the selection of items subject to legal privilege, confidential journalistic material, and sources of journalistic information from data acquired under bulk interception or bulk equipment interference warrants[62].

The IPA provides further safeguards for disclosure of the material overseas and limiting the length of time that data acquired under bulk interception or bulk equipment interference warrants may be retained by a UKIC agency[63].

Bulk interception and bulk equipment interference warrants may only be used to authorise the selection for examination of the content of communications relating to individuals located outside the British Islands. Should it be necessary to examine content acquired under a bulk interception or bulk equipment interference warrant, referable to individuals located inside the British Islands, UKIC must first obtain a targeted examination warrant in relation to that person to carry out such examination[64].

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[65].

Bulk Personal Datasets

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, the majority of whom are not and are unlikely to become of interest to UKIC. Examples might include such a register of electors or a telephone directory.

BPDs are acquired through overt and covert means and in accordance with the Security Service Act 1989 and the Intelligence Services Act 1994. BPDs may be acquired using investigatory powers, from other public-sector bodies or commercially from the private sector. These datasets are typically very large, 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 datasets that have already been acquired to be retained and examined by

[61] Sections 142, 150, 152, 155 IPA for bulk interception and sections 183, 191, 193 and 196 for bulk equipment interference.
[62] Sections 153 and 154, IPA for bulk interception and sections 194 and 195 for bulk equipment interference.
[63] Sections 150 and 151, IPA for bulk interception and sections 191 and 192 for bulk equipment interference.
[64] Section 152 and 193, IPA.
[65] Section 140, IPA for bulk interception and section 179, IPA for bulk equipment interference.

UKIC where it is necessary and proportionate to do so. The provisions create two types of BPD warrant – class BPD warrants and specific BPD warrants:

Class BPD warrants[66] 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[67] 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.

Following a strictly time-limited period of initial examination[68] 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. As with other powers, BPD warrants must be double locked[69].

BPD warrants cannot be issued unless the Secretary of State is satisfied with UKIC's arrangements for storing the BPD and protecting it from unauthorised disclosure.

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.

There are also specific safeguards for health records[70] as well as general safeguards for examination[71].

As with Bulk communications data, 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[72].

Urgent cases

Urgent warrants

For targeted intercept, targeted and bulk equipment interference, and BPD, there are provisions for approval of warrants in urgent cases[73]. These allow for warrants to be approved only by the Secretary of State before the power in question is used in a limited number of

[66] Section 204, IPA.
[67] Section 205, IPA.
[68] Section 220, IPA.
[69] Section 208 IPA.
[70] Section 206, IPA.
[71] Section 221, IPA.
[72] Section 224, IPA.
[73] Sections 24, 109, 180 and 209 IPA, respectively.

circumstances. Urgent warrants can only be used when there is an imminent threat to life or serious harm, or an intelligence or investigative opportunity which is time limited. In these situations, the warrant is still double locked by a Judicial Commissioner, and this has to happen by the third working day after the day on which the warrant was issued.

Should the Judicial Commissioner not approve the warrant within the specified time period, the IPA requires that, as far as is reasonably practicable, anything in the process of being done under the warrant stops as soon as possible[74]. The Judicial Commissioner may direct that any of the material obtained under the warrant is destroyed; impose conditions as to the use or retention of any of that material; in the case of a targeted examination warrant, impose conditions as to the use of any relevant content selected for examination under the warrant.

It should be emphasised that urgent warrants are used in extremely small numbers. For example, in 2020, they accounted for 2% of the applications made by the law enforcement agencies for targeted intercept.[75]

Major modifications made in urgent cases

The IPA also provides a process for major modifications to be made in urgent cases following an adjusted procedure. This applies to targeted intercept, equipment interference, BCD and BPD[76]. In these circumstances, the appropriate person (depending on the type of modification this is either a designated senior official or a Judicial Commissioner) must, before the end of the period ending with the third working day after the day on which the modification was made, decide whether to approve the decision to make the modification and notify the person of their decision.

In cases where the decision is being made by a designated senior official, as soon as is reasonably practicable a Judicial Commissioner must be notified of the decision and, if the senior official has decided to approve the decision to make the modification, the modification in question. The Secretary of State must also be notified of the same points.

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. Schedule 7 of the Act sets out detailed requirements for what the codes must contain.

These codes, which are prepared by the Secretary of State, 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.

[74] Sections 25, 110, 181 and 210 IPA.
[75] IPC's Annual Report 2020, page 86.
[76] Sections 38, 122, 166, 217 IPA respectively.

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.

The Codes set out guidance on the exercise of the powers to which they relate, and those exercising the powers must have regard to them. Whereas a failure to comply with the codes do not itself create criminal or civil liability, it can give rise to a "relevant error" which the organisation responsible must report to IPCO.[77] The codes are also admissible in evidence in court.[78]

Oversight

There are three components of oversight of UKIC:

- Executive oversight, provided by the Secretaries of State and Scottish Ministers;
- Parliamentary oversight, including by the Intelligence and Security Committee of Parliament (ISC);[79]
- Independent judicial oversight, provided by the Investigatory Powers Commissioner (IPC) and his Judicial Commissioners.

Executive oversight

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 (traditionally this has been the Home Secretary for MI5 and the Foreign Secretary for GCHQ and SIS).

[77] See section 235(6) and section 231(9) IPA.
[78] In respect of the status of codes generally, see paragraph 6 of Schedule 7 to the IPA.
[79] https://isc.independent.gov.uk/.

As noted already, under the IPA and related legislation (including Part II of RIPA), the Secretary of State, or in certain circumstances the Scottish Minister, must also personally approve the exercising of all the more intrusive investigatory powers.

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.

Parliamentary oversight

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;[80]
- Statutory Codes of Practice under IPA and related legislation such as RIPA are also subject to Parliamentary approval;
- 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 UKIC is conducted by the ISC – the ISC's role is described below.

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 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.

Members of the ISC 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 ISC is able to request information and documents from UKIC 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,

[80] Parliamentary scrutiny when the IPA was being passed included seven separate Parliamentary reports, a separate review of bulk powers by Lord Anderson KC, the tabling of more than 1,000 amendments, and the taking of more than 2,300 pages of written and oral evidence from stakeholders across society by the Joint Act Committee alone.

including NGOs, other representative bodies and individual members of the public, as well as UKIC.

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.

The ISC also has the power to refer matters to the IPC for investigation.[81]

It should be noted that the ISC's remit does extend beyond just UKIC to cover the intelligence-related work of the Cabinet Office including: the Joint Intelligence Committee; the Assessments Staff; and the National Security Secretariat. The Committee also provides oversight of Defence Intelligence in the Ministry of Defence and the Homeland Security Group in the Home Office.

Section 260 of the IPA required the Secretary of State to prepare a report on the operation of the Act during a six-month period between May 2022 and November 2022 (five years after the Act received Royal Assent). The Act mandates that this report should take account of any other report on the operation of the Act by any Parliamentary Select Committee, and it must be published and laid before Parliament. The Home Office published this report in February 2023[82]. During the preparation of this report, the Home Office consulted the relevant Parliamentary committees, none of whom chose to produce their own reports.

Independent Judicial Oversight

IPCO is the office of the Investigatory Powers Commissioner, a role created by the IPA through the merging of the previous oversight bodies into one single organisation. The previous organisations were the Office of Surveillance Commissioners (OSC), the Interception of Communications Commissioner's Office (IOCCO) and the Intelligence Service Commissioner's Office (ISComm).

The IPC is appointed by the Prime Minister following a joint recommendation by the Lord Chancellor, the Lord Chief Justice of England and Wales, the Lord President of the Court of Session, and the Lord Chief Justice of Northern Ireland. The Prime Minister must also consult

[81] Section 236, IPA.

[82] Home Office report on the operation of the Investigatory Powers Act 2016 (accessible version) - GOV.UK (www.gov.uk).

Scottish Ministers[83]. An individual cannot be appointed as the IPC unless they hold or have held a high judicial office (within the meaning of Part 3 of the Constitutional Reform Act 2005).

Lord Justice Sir Adrian Fulford was appointed as the first IPC in February 2017 by the Prime Minister under section 227(1) of the IPA. 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 (as it then was) and Head of Criminal Justice.

The IPC is supported by a number of Judicial Commissioners. All Judicial Commissioners are senior current or former members of the judiciary and this requirement is included in the IPA[84].

Each Judicial Commissioner (including the IPC) is appointed for three-year terms. They can be reappointed. They cannot be removed from office before the end of the term for which they have been appointed unless a resolution approving the removal has been passed by each House of Parliament. There are limited exceptions to this that allow the Prime Minister to remove them[85].

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

The IPC's main oversight functions are extensive and detailed in legislation.[86] These are regularly reviewed and have recently been updated to ensure all oversight functions have a clear statutory footing.[87]

The role of the Judicial Commissioners includes providing the 'double lock' where use of intrusive powers must be approved both by the Secretary of State (or specified senior officers) and by a Judicial Commissioner.

The 'double lock' means that the Judicial 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.[88] 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 person who made the initial decision to approve the warrant may ask the IPC to reconsider the decision of the Judicial Commissioner, and the IPC's decision will be 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 whether any collateral intrusion into the privacy of third parties has occurred.

---

[83] Section 227, IPA.
[84] Section 227(2) IPA.
[85] Section 228(2) and (5), IPA.
[86] Sections 229 and 230 IPA.
[87] The Investigatory Powers Commissioner (Oversight Functions) Regulations 2022 (legislation.gov.uk).
[88] This review is on judicial review principles, as opposed to a full-merits review. See section 23(2) IPA, for example.

The law allows that in an urgent case, a warrant can be issued before being approved by a Judicial Commissioner. 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[89].

Beyond, their role in the double lock the IPC and his team are responsible for continually inspecting the public authorities who use the investigatory powers. Unlike with other oversight bodies, IPCO conduct their inspections on a proactive rather than reactive basis. In 2022, they conducted 365 inspections, 44 of these were inspections of UKIC. IPCO also publish their inspection statistics throughout the year[90].

IPCO conduct at least one inspection of UKIC on each of the powers in a year (this includes RIPA powers were relevant) as well as cross-cutting safeguards inspections. Nearly all of these are multi-day inspections. Details on these inspections and the reports and recommendations that come from them are covered in IPCO's Annual Reports.

As explained on IPCO's website[91], their teams of specialist inspectors conduct these inspections accompanied by a Judicial Commissioner. Organisations may be inspected by more than one team at multiple visits each year when looking at the use of different investigatory powers. Each of these visits constitutes one inspection.

Inspections are carried out to ensure that when investigatory powers are used:

- compliant authorisations have been given;
- legal requirements (such as necessity and proportionality) have been met;
- Codes of Practice requirements have been adhered to; and
- standards of good practice are maintained.

When completing an inspection, inspectors will visit the authority (either in person or using remote access to the authority's records), review documentation and interview relevant staff members. This could include, for example, interviewing operational and policy teams. Inspectors scrutinise records of the authority's use of an investigatory power. This includes:

- the application for its use;
- the authorisation approving its use;
- applications to renew the authorisation and extend its use; and
- documents cancelling the use of the power.

As well as these fundamental documents, inspectors will review a variety of supporting documents such as risk assessments for covert human intelligence sources or policy logs.

---

89 Sections 24, 109, 180 and 209, IPA.

90 https://www.ipco.org.uk/what-we-do/inspections/inspection-statistics/.

91 Inspections – IPCO.

They will examine training modules and governance structures. Inspectors may also review samples of material obtained through the use of covert powers.

If there is a notable issue at any of the public authorities, picked up either during an inspection or outside it in normal business, IPCO may carry out additional ad hoc inspections as well as their usual scheduled inspections.

The IPC has a statutory obligation to report his findings and activities to the Prime Minister annually.[92] The Prime Minister has an obligation to publish the report and lay a copy of the published report in Parliament. Each of these reports include a specific section on each of the UKIC agencies. The most recent report can be found on IPCO's website[93].

Office for Communications Data Authorisations

The Office for Communications Data Authorisations (OCDA) is IPCO's sister organisation. Like IPCO, OCDA is an independent arm's length body of the Home Office and overseen by the IPC. OCDA was formed in 2018 as a result of the Data Retention and Acquisition Regulations 2018[94] (which amended the Investigatory Powers Act in order to achieve compliance with EU law).

OCDA is responsible for considering nearly all communications data applications made by public authorities in the UK on behalf of the Investigatory Powers Commissioner. During OCDA's operating hours, this also includes CD requests from UKIC for purposes of serious crime only. OCDA's mission is to protect the public using two strands of work:

- protect the human rights of individuals from unjustifiable intrusions by the State, in their capacity as an independent body authorising access to communications data when it is lawful, necessary and proportionate; and
- independently assess, in a professional and efficient manner, the lawful acquisition of communications data by a public authority in order to meet its function of protecting the public[95].

A Framework Agreement from 2021[96], lays out the broad framework for the governance of IPCO and OCDA and how the relationship with the Home Office as the sponsoring department operates.

[92] Section 234 IPA.
[93] Annual Reports – IPCO.
[94] The Data Retention and Acquisition Regulations 2018 (legislation.gov.uk).
[95] OCDA – IPCO.
[96] IPCO-OCDA-Framework-Agreement.pdf (ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com).

Redress

The UK has several independent and well-established redress mechanisms available to individuals who feel they may have been subjected to unlawful surveillance. While challenges to the IPA can be brought through the normal court system, by judicial review e.g. on grounds of illegality, procedural unfairness or irrationality, it is more likely that complaints about the conduct of UKIC pursuant to the use of investigatory powers will be bought before the Investigatory Powers Tribunal[97], which is a specialist tribunal with its own characteristics that distinguish it from other courts and tribunals.

The Tribunal was established by RIPA[98] and replaced the Interception of Communications Act Tribunal, the Security Services Act Tribunal, and the Intelligence Services Act Tribunal. These tribunals were established by the Interception of Communications Act 1985, the Security Service Act 1989 and the Intelligence Services Act 1994 respectively. They demonstrate the UK's long commitment to ensuring specialist judicial redress is available in this space.

The Tribunal provides a right of redress for anyone (regardless of citizenship) who believes they have been a victim of unlawful action by a public authority improperly using covert investigative techniques[99]. Thus, a person in the United States whose personal data is transferred to the territory of the United Kingdom could make a complaint to the Tribunal alleging that UKIC had acted unlawfully in relation to the acquisition or handling of the data.

The Tribunal considers:

- complaints about the use of covert techniques under RIPA, the IPA, the Intelligence Services Act 1994 and the Police Act 1997 against any public authority with investigatory 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.

There are currently 15 Members of the Tribunal, including the President The Right Honourable Lord Justice Singh. IPT members are appointed by His Majesty but following a recommendation by the Secretary of State to the Prime Minister[100].

A person shall not be appointed as a member of the Tribunal unless they hold or have held a high judicial office (within the meaning of Part 3 of the Constitutional Reform Act 2005) or they are or have been a member of the Judicial Committee of the Privy Council. They also need to

[97] https://investigatorypowerstribunal.org.uk/.
[98] Sections 65-70, RIPA.
[99] Section 65(4), RIPA.
[100] Section 95, RIPA.

satisfy the judicial-appointment eligibility condition on a 7-year basis, or be an advocate or solicitor in Scotland of at least seven years' standing, or a member of the Bar of Northern Ireland or solicitor of the Court of Judicature of Northern Ireland of at least seven years' standing[101].

Tribunal members are appointed for five-year periods and are eligible for reappointment. They can be relieved of office by His Majesty at their own request or can be removed from office by His Majesty on an Address presented to Him by both Houses of Parliament. RIPA also lays out the procedure should it be the Scottish Parliament who calls for the removal of a Tribunal member[102].

The Tribunal is unique in that it:

- investigates complaints free of charge and the applicant does not have to hire a lawyer, but can choose to do so at their own expense;
- 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 order, receive, and consider evidence in a variety of forms, even if the evidence may be inadmissible in an ordinary court[103];
- 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[104];
- 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 binding 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;[105]
- 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[106];

[101] Paragraph 1, Schedule 3, RIPA.
[102] Paragraph 1, Schedule 3, RIPA.
[103] Section 68(6), RIPA and rule 13, The Investigatory Powers Tribunal Rules 2018.
[104] Paragraph 4, Schedule 3, IPA.
[105] Section 67(7), RIPA.
[106] Rule 7, The Investigatory Powers Tribunal Rules 2018.

- generally, will not make an order against a losing party for reimbursement of the costs incurred by the opposing party 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;

With effect from 31 December 2018, 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.[107] 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. As of December 2021, the Tribunal had allowed leave to appeal in two cases, one of which, the 'Third Direction' case (IPT/17/86/CH & IPT/17/87/CH), was heard in the Court of Appeal, and dismissed[108].

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. In accordance with the principle of subsidiary, the Strasbourg court may only consider a claim once all routes to domestic remedy have been exhausted.

In November 2022, the Tribunal published a report on its work between 2016 and 2021[109]. In it the Tribunal noted it had seen a 75% increase in the number of complaints between 2017 (202 complaints) and 2021. For 2021, this number was 353. While they do not have a conclusive explanation as to this increase, the Tribunal report suggests that the publicity given to some cases such as the 'Third Direction' case and Wilson v Metropolitan Police (IPT/11/167/H) has increased public awareness in the existence of the Tribunal and confidence in its independence. Additionally, there may have been an impact on 2021 numbers due to the pandemic artificially reducing the 2020 complaints.

When a complaint is made to the Tribunal there are seven possible outcomes:

- No determination;
- Out of jurisdiction;
- Out of time;
- Frivolous and/or vexatious;
- Dismissed/Struck out;
- Withdrawn;
- In favour.

For their 2021 statistics, 43% of complaints were found to be frivolous and 27% vexatious (it should be noted these are only for cases completed that year, there remain ongoing cases that will be reported on at their conclusion). 34% of all complaints were made against UKIC which

[107] Section 67A RIPA, as inserted by the IPA.

[108] IPT Report covering its activities between 2016 and 2021 (published in 2022), page 12 - https://investigatorypowerstribunal.org.uk/wp-content/uploads/2023/03/Report-of-the-Investigatory-Powers-Tribunal-2016-2021.pdf.

[109] TRIBUNAL Report (Tribunal-uk.com).

is broadly consistent with previous years' levels as well. Notification requirements for the complainants and respondents are covered in the Investigatory Powers Tribunal Rules[110].

The Tribunal is restricted in what it can disclose during the investigation of a complaint or claim. The Tribunal Rules[111] state that no information or documents provided to the Tribunal, nor the fact that any have been provided, can be disclosed. Until final determination, therefore, the Tribunal can only inform the complainant that an investigation is ongoing. If the conduct the complainant complained of is found to have occurred, and to have been unlawful, the complainant will receive a determination in their favour. They will then receive as much information as the Tribunal can supply without, where this is relevant, putting national security at risk.

The Tribunal is supported by Counsel to the Tribunal (CTT) as and when required. The Tribunal may appoint CTT to assist the Tribunal's consideration of a complaint in any circumstances the Tribunal considers it appropriate to do so[112]. This includes:

- where a complainant is not legally represented;
- where the respondent objects to the disclosure of evidence;
- where the Tribunal intends to hold a hearing, either in whole or in part, in the absence of the complainant.

The role of CTT is to perform any function that would assist the Tribunal including[113]:

- to identify documents or parts of documents that may be disclosed to a complainant, including making a gist of the non-disclosed part;
- to make submissions to the Tribunal on what documents ought to made available to the complainant and the general public in accordance with the principle of open justice;
- to cross examine witnesses;
- to ensure that all the relevant arguments are placed before the Tribunal.

Counsel must also identify any arguable error of law in relation to any decision or determination made by the Tribunal following a hearing held (in whole or in part) in the absence of the complainant.

[110] The Investigatory Powers Tribunal Rules 2018 (legislation.gov.uk).
[111] Rules 7 and 15, The Investigatory Powers Tribunal Rules 2018.
[112] Rule 12, The Investigatory Powers Tribunal Rules 2018.
[113] Rule 12, The Investigatory Powers Tribunal Rules 2018.

This publication is available from: https://www.gov.uk/government/organisations/department-for-science-innovation-and-technology

If you need a version of this document in a more accessible format, please email alt.formats@dsit.gov.uk. Please tell us what format you need. It will help us if you say what assistive technology you use.