U.S. Department of Justice

National Security Division

Office of the Assistant Attorney General *Washington, D.C. 20530*

Memorandum in Support of Designation of the United Kingdom as a Qualifying State Under Executive Order 14086

Executive Order 14086, signed on October 7, 2022, establishes a two-level redress mechanism for the review of qualifying complaints filed by individuals through an appropriate public authority in a "qualifying state" and alleging certain violations of U.S. law concerning signals intelligence activities. The Attorney General may designate a country or a "regional economic integration organization" as a qualifying state if he determines, in consultation with the Secretary of State, the Secretary of Commerce, and the Director of National Intelligence, that it meets three requirements set forth in section 3(f) of the Executive Order.

This memorandum, prepared by the National Security Division of the Department of Justice, provides information in support of designating the United Kingdom of Great Britain and Northern Ireland and Gibraltar[1] (together the "United Kingdom" or "UK") as a qualifying state, by showing how the United Kingdom meets the three requirements set forth in section 3(f) of Executive Order 14086. Designating the United Kingdom as a qualifying state, so that UK individuals may file complaints through the redress mechanism established by Executive Order 14086, is an essential step for the United Kingdom to grant a "data bridge" to the United States for the United Kingdom Extension to the EU-U.S. Data Privacy Framework ("UK Extension to the EU-U.S. DPF"). The data bridge will in turn permit the transfer under UK law of personal information for commercial purposes from the territory of the United Kingdom to the territory of the United States in reliance on the UK Extension to the EU-U.S. DPF.

I. Determinations to be made to designate a "qualifying state" under Executive Order 14086

Section 3(f) of Executive Order 14086 lists three determinations to be made to designate a country or regional economic integration organization a "qualifying state," followed by three corresponding determinations any one of which may be a basis to revoke or amend a designation:

[1] The United Kingdom has advised that Gibraltar is a British overseas territory for which the United Kingdom is responsible under international law and exercises responsibility with respect to its external affairs, defense and internal security. The safeguards, protections, and administration and supervision of the EU-U.S. Data Privacy Framework will be extended to transfers of personal data from the United Kingdom and Gibraltar to U.S. organizations participating in the UK Extension to the Framework. The United Kingdom has advised that Gibraltar does not have its own investigatory powers legislation or intelligence services and that any signals intelligence activities conducted in Gibraltar by intelligence agencies of the United Kingdom would be governed by the UK laws discussed in this memorandum. For purposes of this memorandum, references to the "United Kingdom" include Gibraltar, in support of designation of the United Kingdom and Gibraltar.

(i) To implement the redress mechanism established by section 3 of this order, the Attorney General is authorized to designate a country or regional economic integration organization as a qualifying state for purposes of the redress mechanism established pursuant to section 3 of this order, effective immediately or on a date specified by the Attorney General, if the Attorney General determines, in consultation with the Secretary of State, the Secretary of Commerce, and the Director, that:

(A) the laws of the country, the regional economic integration organization, or the regional economic integration organization's member countries require appropriate safeguards in the conduct of signals intelligence activities for United States persons' personal information that is transferred from the United States to the territory of the country or a member country of the regional economic integration organization;

(B) the country, the regional economic integration organization, or the regional economic integration organization's member countries of the regional economic integration organization permit, or are anticipated to permit, the transfer of personal information for commercial purposes between the territory of that country or those member countries and the territory of the United States; and

(C) such designation would advance the national interests of the United States.

(ii) The Attorney General may revoke or amend such a designation, effective immediately or on a date specified by the Attorney General, if the Attorney General determines, in consultation with the Secretary of State, the Secretary of Commerce, and the Director, that:

(A) the country, the regional economic integration organization, or the regional economic integration organization's member countries do not provide appropriate safeguards in the conduct of signals intelligence activities for United States persons' personal information that is transferred from the United States to the territory of the country or to a member country of the regional economic integration organization;

(B) the country, the regional economic integration organization, or the regional economic integration organization's member countries do not permit the transfer of personal information for commercial purposes between the territory of that country or those member countries and the territory of the United States; or

(C) such designation is not in the national interests of the United States.

II. Determination that the laws of the United Kingdom require appropriate safeguards for signals intelligence activities affecting U.S. persons

The first determination to be made to designate the United Kingdom, pursuant to section 3(f)(i)(A) of Executive Order 14086, is that the laws of the United Kingdom "require appropriate safeguards in the conduct of signals intelligence activities for United States persons' personal information that is transferred from the United States to the territory" of the United Kingdom. The following discussion describes how the laws of the United Kingdom meet this standard.

As a threshold matter, it is important to note that Executive Order 14086 does not require a "qualifying state" to provide identical or reciprocal safeguards to those provided under U.S. law. Rather, the Executive Order simply calls for a determination that the laws of the qualifying state "require appropriate safeguards." The flexibility inherent in this standard accounts for the fact that different countries, even those sharing democratic values and a commitment to the rule of law, will have legal and national security systems with differing histories and institutions, such that they may legitimately take differing approaches towards enacting privacy safeguards for signals intelligence activities. In other words, the Executive Order's "appropriate safeguards" standard does not impose a rigid "one-size-fits-all" model, but rather asks, in light of the importance of maintaining trust and confidence in the free flow of data in today's networked global economy, whether the laws of a potential qualifying state, when viewed holistically, require appropriate privacy safeguards with respect to its national security activities.

The following discussion analyzes the privacy safeguards required by UK law in the conduct of signals intelligence activities that may affect U.S. persons' personal data, including through the United Kingdom's ratification and adherence to the European Convention on Human Rights. The discussion refers to the report on UK laws governing signals intelligence activities attached to this memorandum (the "UK Report"), which the UK government provides as "evidence submitted by the UK Government to the US Attorney General to support designation as a qualifying state under EO 14086." The discussion below focuses on UK intelligence agencies' potential access to U.S. persons' personal data that has been transferred to the territory of the United Kingdom, with a brief analysis on potential access to data while in transit.[2]

The below analysis demonstrates that the laws of the United Kingdom require comprehensive and detailed safeguards for signals intelligence activities that may affect U.S. persons' personal information. UK safeguards include general requirements for prior approvals (either individually or programmatically) by independent Judicial Commissioners for signals intelligence surveillance including through interception of the content of communications and equipment interference; restrictions on the handling of data acquired; proactive and well-resourced oversight by the Investigatory Powers Commissioner's Office; and a well-established

[2] This approach was also adopted in the memorandum published in support of designation by the Attorney General of the European Union and other countries of the European Economic Area. The primary basis for this approach is that a destination country's laws and practices regarding signals intelligence activities do not uniquely govern the privacy protection that is afforded to data located outside of that country or outside of any country, as explained further in that EU/EEA memorandum and also below in section II.b.v. Department of Justice, National Security Division, *Memorandum in Support of Designation of the European Union and Iceland, Liechtenstein and Norway as Qualifying States Under Executive Order 14086*, at 13-14, available at https://www.justice.gov/opcl/executive-order-14086 ("NSD Supporting Memorandum for Designation of the EU/EEA").

path to judicial redress for individual complainants through the Investigatory Powers Tribunal. To be sure, there are areas of divergence between the laws of the United States and the laws of the United Kingdom, including for example certain UK surveillance authorities that are not available in U.S. law, such as UK authorization for bulk intelligence collection domestically. However, the strong safeguards embedded throughout the UK legal regime, including querying limitations and documentation requirements with respect to its domestic bulk collection, demonstrate its clear commitment to the protection of privacy with respect to its national security activities. In this connection, it is notable that the United Kingdom and the United States have both signed the 2022 OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, which sets forth principles for protecting privacy during government access to data for law enforcement and national security purposes, describing the legal protections for privacy that both states share in connection with these activities. In that OECD Declaration, the United States affirms that it takes into account a destination country's effective implementation of the Declaration's principles as a positive contribution towards facilitating transborder data flows.

Based on this analysis, as well as the deferential "appropriate safeguards" standard in Executive Order 14086, and the importance of commercial transfers of data between the United Kingdom and the United States, it is within the Attorney General's discretion to conclude, in consultation with the Secretary of State, the Secretary of Commerce, and the Director of National Intelligence, that the laws of the United Kingdom require appropriate safeguards for purposes of a section 3(f)(i)(A) determination.

a. The European Convention on Human Rights

The United Kingdom is a contracting party to the European Convention on Human Rights ("ECHR"), which establishes the European Court for Human Rights ("ECtHR"). The jurisdiction of the ECtHR extends, according to article 32 of the ECHR, to all matters concerning its interpretation and application. Regarding interferences with privacy, article 8 mandates that "[e]veryone has the right to respect for his private and family life, his home and his correspondence," with a proviso for government interference stating that "there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

The ECtHR has identified several categories of "minimum safeguards" that ECHR contracting parties must adopt to ensure effective safeguards against abuse of government powers to access electronic communications for national security purposes. These categories of minimum safeguards identified by the ECtHR are similar on the whole to the safeguards adopted in section 2(c) of Executive Order 14086. They include the grounds for authorizing surveillance; the categories of people liable to have their communications accessed; procedures for examining, using, storing, retaining, and erasing the data obtained; procedures for preserving the integrity and confidentiality of data; precautions to be taken when communicating the data to other parties; arrangements for supervising the implementation of surveillance measures and

compliance with safeguards; and the remedies provided for by national law.[3] *See Roman Zakharov v. Russia*, Application no. 47143/06, §§ 233-34 (2015); *Kennedy v. United Kingdom*, Application no. 26839/05, §§ 152-53 (2010); *Weber and Saravia v. Germany*, Application no. 54934/00, § 95 (2006); see discussion at *Centrum För Rättvisa v. the Kingdom of Sweden*, Application no. 35252/08, §§ 249-55 (2021). The ECtHR has also found it important for domestic law to require intercepting agencies to keep records of interceptions, in order to ensure that supervisory bodies have effective access to details of surveillance activities undertaken. *Roman Zakharov v. Russia*, § 272; *Big Brother Watch and Others v. the United Kingdom*, Application nos. 58170/13, 62322/14 and 24960/15, § 356 (2021).

In our earlier memorandum we assessed that the legal requirements imposed by the ECHR on the countries of the European Union and European Economic Area provided a sufficient basis for a section 3(f)(i)(A) determination, noting that the categories of "minimum safeguards" that the ECtHR has identified for signals intelligence activities are on the whole similar both to the principles for protecting privacy in the 2022 OECD Declaration on Government Access to Personal Data Held by Private Sector Entities and the safeguards in Executive Order 14086 and other U.S. law.[4] We also noted, however, that the jurisprudence of the ECtHR indicates what precise safeguards are required with respect to only some of the categories of "minimum safeguards," while for other categories the ECtHR appears not to have specified the precise safeguards that are required, either because the ECtHR has not had occasion to do so or because the ECtHR leaves those issues to ECHR member countries' discretion.[5]

The ECtHR has applied the ECHR to review the surveillance laws of the United Kingdom on several occasions, and Parliament has since enacted legislation incorporating the requirements of these ECtHR decisions, in addition to establishing other limitations and safeguards.[6] *E.g.*, *Big Brother Watch and Others v. the United Kingdom* (ruling, *inter alia*, that the requirements of article 8 of the Convention were not met by the authorizations in the Regulation of Investigatory Powers Act 2000 for bulk interception of electronic communications within the United Kingdom or for acquisition of non-content communications data); *Kennedy v. United Kingdom* (ruling that the requirements of article 8 were met by the safeguards in the Regulation of Investigatory Powers Act 2000 for surveillance of domestic electronic communications relating to restrictions on acquisition and post-acquisition handling of data, oversight of intelligence agencies' compliance with those restrictions, and individualized redress through the Investigatory Powers Tribunal); *Liberty v. United Kingdom*, Application no. 58243/00 (2008) (ruling that the surveillance of electronic communications authorized by the Interception of Communications Act 1985 violated article 8 including by not publicizing procedures for retention, deletion, dissemination, and querying of intercepted material); *Malone*

[3] The categories of "minimum safeguards" identified by the ECHR for intelligence surveillance activities, and the requirements established by the ECtHR for each of the categories, are discussed in more detail in the memorandum published in support of designation by the Attorney General of the European Union and other countries of the European Economic Area. NSD Supporting Memorandum for Designation of the EU/EEA at 5-11.
[4] *Id.* at 32.
[5] *Id.* at 10-11.
[6] For example, the deficiencies identified in the *Big Brother Watch* judgment of the ECtHR were largely addressed through the introduction of the Investigatory Powers Act 2016, which primarily updated the Regulation of Investigatory Powers Act 2000 (RIPA) regime, and further legislative changes have since been made to bring the UK regime into line with that judgment.

v. United Kingdom, Application no. 8691/79 (1984) (ruling that authorizations for surveillance of communications by police did not clarify sufficiently the discretion granted to public authorities).

b. UK laws on signals intelligence activities and related privacy safeguards

The primary UK legislation governing signals intelligence activities and establishing related privacy safeguards is the Investigatory Powers Act 2016 ("IPA"). As explained in the attached UK Report, if a U.S. person's personal information has been transferred from the United States to an organization in the United Kingdom, the UK government may compel the UK organization to disclose the U.S. person's personal data for intelligence purposes only where authorized by the IPA and within the statutory functions of the UK intelligence community. The statutory functions of the three organizations comprising the UK intelligence community—Military Intelligence 5 ("MI5"), Military Intelligence 6 ("MI6," the Secret Intelligence Service or "SIS"), and Government Communications Headquarters ("GCHQ") (collectively the "UKIC")—are set out in the Security Services Act 1989 and the Intelligence Services Act 1994. While there is some variation among these three organizations, their collective purpose can be summarized, according to the UK Report, as protecting national security and the economic well-being of the United Kingdom and supporting the prevention and detection of serious crime.

The IPA establishes the Investigatory Powers Commissioner ("IPC") who is responsible for exercising independent review and oversight of, among other areas, the UKIC's use of the IPA's powers. The IPC Office ("IPCO") includes the IPC's staff of Judicial Commissioners, along with inspectors, lawyers, and communications experts. The IPC and the Judicial Commissioners are appointed by the Prime Minister for three-year, renewable terms, upon joint recommendation by a group of four senior officials, three of whom are themselves judicial officials independent of the government. IPA §§ 227(1)-(4); 228(2), (3). A candidate for appointment must be a person who "holds or has held a high judicial office," *id.* §§ 227(2), which means a candidate will in almost all cases[7] have been selected by the Judicial Appointments Commission, a body independent of Government which selects individuals to serve as judges in senior judicial positions, based solely on merit, selecting only persons of good character, having regard for the need to encourage diversity in the range of people available for selection.[8] They are removable only by resolution passed by each House of Parliament or by the Prime Minister if a Commissioner has been the subject of specified legal actions, such as a criminal conviction or a bankruptcy order. *Id.* § 228(4)-(5).

The IPA authorizes several types of surveillance powers, as discussed below, and establishes the privacy safeguards for the UKIC's use of those powers. IPA warrants authorizing intelligence surveillance are subject to prior review and approval, as well as subsequent oversight, by the Judicial Commissioners in the IPCO. Approval by Judicial Commissioners is

[7] The exception is appointees to the Supreme Court who had not previously held high judicial office, as Supreme Court Justices are selected not by the Judicial Appointments Commission, but instead by a commission comprising a Justice of the Supreme Court and a member of each of the judicial appointment bodies of England and Wales, Scotland, and Northern Ireland.

[8] More information on the Judicial Appointments Commission is available at http://www.judicialappointments.gov.uk/ .

the second step of the so-called "double lock" mechanism for approval of warrants, following initial approval by the Secretary of State (or specified senior officer). Pursuant to relevant sections of the IPA, the Judicial Commissioner applies the same principles that would be applied by a court on an application for judicial review and must consider, among other things, whether a warrant is necessary for the purpose stated and proportionate to what is expected to be achieved. If the Judicial Commissioner is not satisfied that the requirements of the IPA have been met, the warrant may not be issued and no action may be taken on the basis of it. The official who made the initial decision to approve the warrant may ask the IPC to reconsider a denial by a Judicial Commissioner, and the IPC's decision is final.

The different IPA surveillance powers are accompanied by Codes of Practice that provide guidance on how the powers may be used. The Codes of Practice, which are publicly available, are prepared by the Secretary of State, are subject to public consultation, and must be reviewed and approved by both Houses of Parliament. IPA Schedule 7 sets out detailed requirements for what the codes must contain, including, for example, relevant definitions, guidance on general considerations around the application of principles of necessity and proportionality, processes for seeking a warrant or authorizations, and other guidance. Although failure to comply with a Code of Practice is not itself a basis for criminal or civil liability, it may be taken into account by courts, the IPC, and the Investigatory Powers Tribunal, and it can give rise to a "relevant error" which the UKIC agency must report to the IPC. IPA §§ 235(6), 231(9), sched. 7 § 6(4)-(5). Codes of Practice are also admissible as evidence in court. *Id.* sched. 7 § 6(3).

In addition, the IPA requires that each "public authority" who issues a warrant (i.e., the Secretary of State on behalf of the UKIC) or approves a decision to issue a warrant (i.e., a Judicial Commissioner) must have regard to specified privacy considerations. The authority must have regard to "whether what is sought to be achieved by the warrant . . . could reasonably be achieved by other less intrusive means; whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant . . . is higher because of the particular sensitivity of that information; the public interest in the integrity and security of telecommunication systems and postal services; and any other aspects of the public interest in the protection of privacy." IPA § 2(2). Those considerations are subject to other specified considerations, such as the interests of national security of the United Kingdom and the public interest in preventing or detecting serious crime. *Id.* § 2(4).

The following sections describe the different types of signals intelligence collection activities authorized by the IPA. As in the United States under the Foreign Intelligence Surveillance Act, an independent judicial officer is generally required to provide *ex ante* approval, either for each individual target or at a programmatic level, for all IPA surveillance involving acquisition of the content of communications. Following the discussion of IPA collection authorities is a discussion of privacy safeguards relating to collection and handling of the data acquired, IPCO oversight, and individualized redress.

i. Intelligence collection activities authorized by the IPA and related safeguards

a) Targeted intelligence surveillance

The IPA authorizes three types of targeted intelligence surveillance. Two require warrants. First, part 2 of the IPA authorizes intercept warrants for the targeted interception of the content of electronic communications in the course of their transmission through telecommunications networks, including with the assistance of a private company. Targeted intercept warrants may be used to obtain access to stored data or real-time communications. Second, part 5 of the IPA authorizes equipment interference warrants for the targeted acquisition of the content of electronic communications and related data through a range of techniques carried out either remotely or by physically interacting with equipment including traditional computers or computer-like devices, including through unilateral covert access. *See* Equipment Interference Code of Practice ("EI CoP") ¶¶ 3.2-3.3. Third, part 3 of the IPA authorizes through non-warrant approvals the targeted acquisition of non-content "communications data" generated by telecommunications operators and service providers in the course of their business. For each of these three types of targeted surveillance, the IPA identifies the public authorities, including law enforcement and intelligence agencies, that may apply for warrants or other approvals. IPA §§ 18, 70, 73, 102-07.

Where warrants are required—for the targeted interception of communications content and targeted equipment interference—the IPA implements the "double lock" mechanism, establishing the legal standard that must be met for the Secretary of State to issue the warrant on behalf of a UKIC, and then requiring that the warrant be reviewed and approved by an independent Judicial Commissioner before it may take effect or, in emergency situations, within three working days of the warrant's issuance. IPA §§ 19-25, 102-110. The Judicial Commissioner must review the warrant to confirm that the interception or equipment interference it would authorize is necessary based on the specified purpose and that the conduct the warrant authorizes is proportionate to what is sought to be achieved. *Id.* §§ 23, 108. In contrast to the provisions in section 2(b) of Executive Order 14086 which lists the specific legitimate objectives in pursuit of which U.S. signals intelligence activities may be conducted, the purposes for which IPA warrants can be issued are stated more broadly, in terms of the three objectives of national security, preventing or detecting serious crime, and the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security. *Id.* §§ 19-20, 102. The IPA also requires that these two types of warrants specify or describe, depending on the type of warrant and information sought, the "factors," (analogous to the specification of "selectors" in U.S. law and practice) such as the addresses, numbers, or apparatus, that will be used to identify communications likely to be from or intended for the persons, organizations, or premises named or described in the warrant, the equipment to be accessed, or other description of the nature of the investigation and the activities that would be authorized. *Id.* § 31(8), 115. Codes of Practice set out in further detail the information to be provided by an agency when seeking a warrant—including background on the investigation, names or descriptions of targets of surveillance where reasonably practicable, and a description of the conduct to be authorized by the warrant and why it is proportionate to what is sought to be achieved, including whether what is sought to be achieved by the warrant could reasonably be achieved by other less intrusive means—and also the matters that the Secretary of State must

consider when deciding whether or not to issue the warrant. Interception of Communications Code of Practice ("IoC CoP") ¶¶ 5.29-5.30; EI CoP ¶¶ 5.34-5.35.

Targeted interception and equipment interference warrants may target the communications of particular persons or a single set of premises or the equipment of particular persons, or they may be issued as "thematic" warrants that target a group of persons carrying out a particular activity or sharing a common purpose, such as an organized crime group, or that authorize multiple equipment interferences or related activities for the purposes of a single investigation or operation. IPA §§ 17(2), 31(4)-(5), 101(1)(c), (e)-(f); *see* IoC CoP ¶¶ 5.6-5.11; EI CoP ¶¶ 5.12-5.14. Thematic warrants must describe the purpose or activity shared by the group of persons or organizations subject to surveillance or the investigation or operation for the purposes of which the warrant authorizes surveillance of more than one person or organization or more than one set of premises. Thematic warrants are appropriate "where a series of individual warrants is not practicable" or where otherwise suitable given "operational circumstances," and they may only be issued where the Judicial Commissioner has sufficient foresight of the interference with privacy to allow a proper decision as to the necessity and proportionality of the conduct to be authorized. IoC CoP ¶¶ 5.11, 5.17-5.18; EI CoP ¶¶ 5.13, 5.20-5.21.

Unlike traditional FISA surveillance in which the targeting of each specific individual is reviewed and approved by the FISA court, after approval by a Judicial Commissioner of a targeted interception warrant, the scope of the warranted surveillance may be modified through either "major" or "minor" modifications. IPA §§ 34-37. Major modifications relate to the adding or varying of a name or description of a person, or group of persons, or organization or set of premises to which the warrant relates. Major modifications may be made only by either the Secretary of State (or Scottish Ministers) or a senior official acting on their behalf. *Id.* § 35(1). Minor modifications relate to removing the name or description of a person or group of persons or organization or set of premises, or to the adding, varying or removing of a factor specified in the warrant, for example a target's phone number or email address. *Id.* § 34(2), (5). Minor modifications may be made by the person to whom the warrant is addressed, or a person holding a senior position within that public authority. *Id.* § 35(2). Equipment interference warrants may similarly be modified by adding, varying or removing the names or descriptions in the warrant including of the type of equipment to which the warrant relates. *Id.* § 118. Modifications to equipment interference warrants may be made only by the Secretary of State (or Scottish Ministers) or a senior official acting on their behalf. *Id.* § 119. A Judicial Commissioner must be notified of major modifications to targeted interception warrants, and of all modifications to targeted equipment interference warrants (other than removals of equipment to which the warrant relates), which notifications may lead to inquiries from Judicial Commissioners pursuant to their oversight functions discussed below. *Id.* §§ 37, 121.

The third type of targeted surveillance power, acquisition of non-content communications data, does not require a warrant but does require approval by the Office for Communications Data Authorizations ("OCDA"), an independent arm's length body of the Home Office that is overseen by the IPC. The IPC delegates his powers to OCDA's authorizing officers who then make independent decisions on whether to grant or refuse communications data requests, ensuring that all requests are lawful, necessary and proportionate. IPA § 238(5). The list of authorized purposes for the acquisition of communications data includes the same purposes as

for the warranted surveillance discussed above along with additional purposes including public safety, preventing death or injury, and assisting investigations into alleged miscarriages of justice. *Id.* § 60A(7). Communications data authorizations must be issued based on findings that the authorization is necessary based on the specified purpose and that the conduct authorized is proportionate to what is sought to be achieved, *id.* §§ 60A(1), 61(1), and that communications data authorizations specify or describe the non-content data to be obtained, *id.* § 64(1)(d). The UKIC must obtain OCDA approval for acquisitions of communications data that relate solely to serious crime, other than in urgent circumstances. *Id.* sched. 4. The UK Report explains that because OCDA operates only during regular office hours, the UKIC may need to be able to access targeted communications data at all hours in urgent situations. Therefore, for applications for authorizations seeking access to communications that are urgent and relate solely to serious crime, as well as for applications that are not related solely to serious crime, the UKIC may acquire communications data on the basis of an internal authorization process, which requires authorization by a member of the senior civil service or above. *Id.* §§ 61, 61A(7), sched. 4. The IPC, supported by IPCO, in turn provides oversight, as discussed in more detail below, of OCDA and of the broader IPA regime for the acquisition of non-content communications data.

b) Warrants for foreign-focused bulk surveillance

A particularly relevant factor for purposes of reviewing, pursuant to section 3(f)(i)(A) of Executive Order 14086, whether the laws of the United Kingdom "require appropriate safeguards in the conduct of signals intelligence activities for United States persons' personal information that is transferred" from the United States to the United Kingdom, are the safeguards that are required under UK law for surveillance focused on communications sent or received outside the United Kingdom. As discussed in the supporting memorandum for designation of the EU/EEA, a number of European countries have established special "foreign-focused" surveillance programs within their territories focused on monitoring and gathering electronic communications sent from or received abroad, which are subject to privacy safeguards that differ from the safeguards applicable to intelligence surveillance of domestic communications.[9] Similarly, the United States has also established a program for foreign-focused intelligence surveillance within U.S. territory, through Section 702 of the Foreign Intelligence Surveillance Act ("FISA") which authorizes the U.S. government to acquire electronic communications sent or received by non-U.S. persons located outside the United States to acquire foreign intelligence information.

The IPA authorizes two types of such foreign-focused surveillance, both of which operate through warrants authorizing acquisition of data in bulk. In this respect, these UK programs differ from the U.S. program for foreign-focused intelligence surveillance under FISA Section 702, which authorizes acquisition of the electronic communications only of specifically targeted persons.[10] These two types of bulk warrant authorizations under the IPA correspond to the two types of targeted warrants discussed above—one for interception of the content of

[9] NSD Supporting Memorandum for Designation of the EU/EEA at 16-19.

[10] While Section 702 safeguards differ from the individualized court approvals required under other sections of FISA for electronic surveillance of persons located in the United States, the Section 702 program operates only on a targeted basis, authorizing the acquisition of the electronic communications of specific persons based on written justifications, with each individual targeting decision and rationale reviewed through independent oversight. *See id.*

communications and the other equipment interference. Specifically, chapter 1 of part 6 of the IPA authorizes warrants for the bulk interception of the content of communications, and chapter 3 of part 6 authorizes warrants for bulk equipment interference. Each of these warrants is "foreign-focused" in the sense described above because it may only be used for the "main purpose" of obtaining information relating to "overseas-related" communications or information, meaning communications sent or received by, or information about, individuals located outside the British Islands. IPA §§ 136(2)-(3); 176(1)-(3). These IPA warrants thus could in principle be used by the UKIC for the purpose of acquiring electronic communications sent or received by a U.S. person in the United States that are sent to or from a person in the United Kingdom or that are passing through the United Kingdom.

As with all IPA warrants, these foreign-focused bulk warrants are subject to the "double lock" mechanism including prior approval by a Judicial Commissioner. The Secretary of State must confirm, among other things, that the purpose of a warrant must always include national security, possibly in combination with the purpose of countering serious crime or of advancing the economic well-being of the United Kingdom, and that the warrant is necessary for those purposes and the conduct authorized is proportionate to what is sought to be achieved by the conduct. IPA §§ 138(1)(b)-(c), (2); 178(1)(b)-(c), (2). Codes of Practice set out in detail the information to be provided when seeking a warrant, and also the matters that the Secretary of State must consider when deciding whether or not to issue the warrant, including an explanation of why what is sought to be achieved could not reasonably be achieved by other less intrusive means. IoC CoP ¶¶ 6.17-20; EI CoP ¶¶ 6.10-13. A Judicial Commissioner must review the Secretary of State's conclusions as to necessity and proportionality and other matters. IPA §§ 140(1); 179(1). Bulk acquisitions of material through these warrants enable the UKIC to establish links between known subjects of interest and search for traces of activity that may indicate a threat to the United Kingdom. The Codes of Practice state that in practice, bulk interception of communications typically uses several different processing systems with filtering to select the types of communications of intelligence value, so that a significant proportion of the communications are automatically discarded; bulk equipment interference also typically involves filtering or processing at or soon after the point of collection. IoC CoP ¶¶ 6.4-6.6; EI CoP ¶ 6.5.

While the United Kingdom, unlike the United States, authorizes domestic collection of data in bulk for intelligence purposes,[11] UK law restricts the querying, or "selection for examination" of the information acquired through bulk interception and bulk equipment interference warrants. The Secretary of State is required to confirm in the warrant that arrangements are in force to ensure that the selection for examination of any material obtained

[11] U.S. law prohibits bulk data collection domestically for intelligence purposes. The EO 14086 provisions governing bulk collection pertain to extraterritorial signals intelligence activities. Under U.S. law, after personal data has been transferred from the United Kingdom to a private company in the United States, U.S. intelligence agencies may compel the company to disclose the data for national security purposes only based on statutes authorizing such access, which are limited to the FISA statute, discussed above, and the "national security letter" statutes, such as section 2709 of the Electronic Communications Privacy Act, which authorize administrative requests for information not including the content of communications. Demands under FISA or through national security letters may be issued by U.S. intelligence agencies only on a targeted basis and do not permit bulk collection. *See* Letter from Christopher C. Fonzone, ODNI General Counsel (9 December 2022), annexed to the European Commission's adequacy decision for the United States, at 3-4 (reviewing statutory prohibitions on bulk collection for data acquisition authorized in the FISA statute and in the statutes authorizing national security letters).

under the warrant is carried out only for the purposes specified in the warrant and only where necessary and proportionate in all the circumstances. IPA §§ 150(1)(b), 152(1); 191(1)(b), 193(1). The Judicial Commissioner must, along with confirming that the warrant is necessary and proportionate, confirm that the warrant specifies the operational purposes for which examination of the data acquired is necessary, drawing from a list of purposes maintained by the UKIC and reviewed by the Prime Minister annually and shared every three months with the Intelligence and Security Committee of Parliament. *Id.* §§ 140(1)(c), 142; 179(1)(c), 183. The operational purposes must be specified in greater detail than the relevant statutory grounds, and must describe a clear requirement and contain sufficient detail to satisfy the Secretary of State that intercepted content or secondary data may only be selected for examination for specific reasons. IoC CoP ¶ 6.62; EI CoP ¶ 6.69. After a warrant is issued it may be modified by specifying additional operational purposes justifying selection for examination of the material collected, or by varying the equipment interference conduct authorized by the warrant, but only with the approval of a Judicial Commissioner. IPA §§ 145-46; 186-87. Material should be selected for examination only by authorized persons who receive regular mandatory training regarding IPA requirements, specifically the requirements of necessity and proportionality. IoC CoP ¶ 6.73; EI CoP ¶ 6.77. To enable effective oversight, documentation must be created and retained for each selection for examination showing why access to the material is necessary and proportionate and the applicable operational purposes, with a mechanism preventing access, to the extent possible, unless such documentation has been created. IoC CoP ¶ 6.74; EI CoP ¶ 6.78. Periodic compliance audits should be carried out to ensure compliance with all legal safeguards, including to ensure that the required documentation justifying selection for examination has been correctly compiled, with any breaches of safeguards to be reported to the Investigatory Powers Commissioner. IoC CoP ¶ 6.76; EI CoP ¶ 6.80. The IPC is under a duty to review the adequacy of these safeguards. IoC CoP ¶ 6.77; EI CoP ¶ 6.81.

c) Warrants for bulk collection of non-content communications data

UK law separately authorizes bulk intelligence surveillance domestically of non-content communications data. Chapter 2 of IPA part 6 authorizes warrants for the UKIC to acquire non-content communications data in bulk from a telecommunications operator, which includes any person who offers or provides a telecommunications service to persons in the United Kingdom or who controls or provides a telecommunication system which is (wholly or partly) in or controlled from the United Kingdom. IPA §§ 158(5)-(6), 261(10). A bulk acquisition warrant may authorize the collection of stored or real-time data. Bulk Acquisitions of Communication Data Code of Practice ("BAC CoP") ¶ 3.3. In contrast to the bulk powers discussed above under chapters 1 and 3 of Part 6 of the Act, which must be focused on communications of persons outside the UK, a bulk acquisition warrant may authorize the collection of non-content communications data in relation to individuals both inside and outside the UK.

As with all IPA warrants, bulk acquisition warrants are subject to the "double lock" mechanism including prior approval by a Judicial Commissioner. The Secretary of State must confirm, among other things, that the warrant is necessary for purposes including national security, possibly in combination with the purpose of countering serious crime or of advancing the economic well-being of the United Kingdom, and that the conduct authorized by the warrant is proportionate to what is sought to be achieved by that conduct. IPA §§ 158(1)(a)-(b), (2), (3).

The relevant Code of Practice sets out in detail the information to be provided when seeking a warrant and the matters that the Secretary of State must consider when deciding whether or not to issue the warrant, including an explanation of why what is sought to be achieved could not reasonably be achieved by other less intrusive means. BAC CoP ¶¶ 4.1-4.5. A Judicial Commissioner must review the Secretary of State's conclusions as to necessity and proportionality and other matters. IPA § 159(1). The Code of Practice also recognizes that the analysis of non-content communications data obtained in bulk is a primary means by which UKIC agencies are able to discover and assess threats to the United Kingdom, which can only be achieved effectively through aggregating data from a wide range of sources acquired under multiple bulk warrants, not limited to non-content communications data acquired in bulk, and that this analysis allows the UKIC to draw together fragments of information into coherent patterns, which allow for the identification of those threats while at the same time minimizing intrusion into privacy. BAC CoP ¶ 6.11.

Again here, while the United Kingdom, unlike the United States, authorizes domestic collection of data in bulk for intelligence purposes, UK law restricts the querying, or "selection for examination" of the material acquired in bulk. As with the foreign-focused bulk warrants discussed above, these warrants for bulk acquisition of non-content communications data must specify safeguards for the querying or "selection for examination" of the information acquired in bulk. The Secretary of State is required to confirm in the warrant that arrangements are in force to ensure that the selection for examination of any material obtained under the warrant is carried out only for the purposes specified in the warrant and only where necessary and proportionate in all the circumstances. IPA §§ 158(1)(c), 172(1). A Judicial Commissioner must, along with confirming that the warrant is necessary and proportionate, confirm that the warrant specifies the operational purposes for which examination of the data acquired is necessary, drawing from a list of purposes maintained by the UKIC and reviewed by the Prime Minister annually and shared every three months with the Intelligence and Security Committee of Parliament. *Id.* §§ 159(1)(c), 161. The operational purposes must be specified in greater detail than the relevant statutory grounds, and must describe a clear requirement and contain sufficient detail to satisfy the Secretary of State that intercepted content or secondary data may only be selected for examination for specific reasons. BAC CoP ¶ 6.6. After a warrant is issued it may be modified by specifying additional operational purposes justifying selection for examination of the material collected, but only with the approval of a Judicial Commissioner. IPA §§ 164-65. To enable effective oversight, documentation must be created and retained for each selection for examination showing why access to the material is necessary and proportionate and the applicable operational purposes. BAC CoP ¶ 6.15. The relevant Code of Practice specifies that periodic compliance audits should be carried out to ensure that the documentation justifying selection for examination has been correctly compiled, with any breaches of safeguards to be reported to the Investigatory Powers Commissioner. *Id.* ¶ 6.16. The IPC is under a duty to review the adequacy of these safeguards. *Id.* ¶ 6.17.

d) Retention and examination of bulk personal datasets

Part 7 of the IPA authorizes warrants for a UKIC agency to retain and examine bulk personal datasets ("BPDs") that the agency has obtained under the IPA or based on separate statutory authority. A 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 the UKIC. IPA § 199(1)(b). The UK Report advises that examples might include a register of electors, a telephone directory, or a database of travel information.

BPDs may be initially acquired based on several separate statutory authorities, through overt and covert means. These may include authorities under the Security Service Act 1989 and the Intelligence Services Act 1994 ("ISA") for UKIC agencies to obtain information where necessary for the proper discharge of their statutory functions. *See* Bulk Personal Data Code of Practice ("BPD CoP") Annex 1. BPDs may also be acquired under the authority of warrants issued under section 5 of the ISA relating to property interference otherwise than for the purposes of obtaining communications, under the authority of covert human intelligence operations authorized under section 29 of the Regulation of Investigatory Powers Act 2000 ("RIPA"), and other authorities. *See id.* ¶¶ 2.11-2.13. The UK Report indicates that BPDs may also be acquired from other public-sector bodies or commercially from the private sector.

UK law in this regard imposes a more stringent requirement than in the United States, where intelligence agencies are generally not required to obtain independent authorization to query or otherwise utilize datasets that have been lawfully acquired. In the United Kingdom, after such datasets have been acquired, they may be retained and examined by UKIC agencies only based on the IPA "double lock" warrant requirement. Warrants may be issued either for a "class" of BPDs or for a specific BPD. IPA § 200(3). The Secretary of State may issue a warrant where necessary for specified purposes including national security, prevention of serious crime, or the UK's economic well-being where relevant to national security; where the conduct authorized by the warrant is proportionate to what is sought to be achieved by the conduct; and where the warrant specifies the purposes for which examination of the data is necessary, drawing from a list of purposes maintained by the UKIC and reviewed by the Prime Minister annually and shared every three months with the Intelligence and Security Committee of Parliament; and other criteria are met relating to secure storage of the BPD. *Id.* §§ 204(3), 205(6), 212. The relevant Code of Practice provides further guidance and elaboration on statutory criteria for warrant, including restrictions for certain categories of protected data. BPD CoP ¶¶ 4.1-4.58. A Judicial Commissioner must review the Secretary of State's conclusions relating to necessity, proportionality, and selection for examination. IPA § 208.

The IPA provides for a UKIC agency to undertake a time-limited (three or six months) initial examination of a BPD to determine whether it has intelligence or investigative value and it would be necessary and proportionate to retain and examine it under a warrant. IPA § 220. This initial examination must be only for those preliminary purposes and not for actual intelligence operations. BPD CoP ¶¶ 2.4-2.5. If a warrant for retention and examination is issued, the Secretary of State must ensure for each BPD warrant that arrangements are in place for ensuring that selection of data for examination is carried out only for operational purposes specified in the warrant and where necessary and proportionate in all the circumstances. IPA § 221(1). To enable effective oversight, documentation must be created and retained for each selection for examination showing why access to the material is necessary and proportionate and the applicable operational purposes. BPD CoP ¶ 7.7. The relevant Code of Practice specifies that periodic compliance audits should be carried out including to ensure that the documentation justifying selection for examination has been correctly compiled, with any breaches of

safeguards to be reported to the IPC. *Id.* ¶ 7.8. UKIC arrangements for access to BPDs will be kept under review by the IPC. *Id.* ¶ 7.6.

ii. Post-Acquisition Handling of Data

The IPA and the Codes of Practice contain detailed provisions for the handling of information acquired by the UKIC under the authority of IPA warrants. Each of the types of warrants discussed above require that the Secretary of State ensure that satisfactory arrangements are in place for safeguards relating to the post-acquisition handling of the information to be acquired. IPA §§ 19(3)(c); 104(1)(c); 138(1)(e); 158(1)(d); 178(1)(e). Specifically, for each of the types of warrants discussed above, relevant IPA provisions identify entities authorized to access data collected, require secure storage of material acquired under warrants, and require that access to and disclosure and copying of material be limited to the minimum extent necessary for authorized purposes. *Id.* §§ 53(2)-(5); 129(2)-(5); 150(2)-(5); 171(2)-(5); 191(2)-(5).

Regarding the retention and destruction of data acquired, the IPA requires that the data be destroyed when there are no longer any relevant grounds for retaining the data. *Id.* Standards and procedures for implementation of this standard are set out in the Codes of Practice. For example, any material retained as relevant should be periodically reviewed for continuing relevancy. IoC CoP ¶ 9.23; EI CoP ¶ 9.30. For data that was acquired in bulk, a UKIC agency must specify maximum retention periods for different categories of data reflecting its nature and intrusiveness, which normally should not be longer than two years, and which should be agreed with the IPC. IoC CoP ¶ 9.24; EI CoP ¶ 9.31.

Regarding the dissemination of data acquired, the Codes of Practice likewise further develop the IPA standard that material obtained under interception warrants may only be disclosed to the minimum extent necessary. The Codes of Practice recognize that "data will need to be disseminated both within and between intercepting authorities, as well as to consumers of intelligence (which includes oversight bodies, the Secretary of State etc.)." IoC CoP ¶ 9.15; EI CoP ¶ 9.22. The guiding standards are the prohibition of disclosure to persons who have not been appropriately vetted and the "need-to-know" principle. *Id.* In accordance with these standards, it may be necessary for a UKIC agency to disclose material obtained under a warrant to another UKIC agency, or to a police agency in response to a request for assistance in relation to an investigation or operation. IoC CoP ¶ 9.15; EI CoP ¶ 9.23. Such requests for assistance may require the selection of bulk intercepted material for examination either for target discovery to generate leads, or to further investigate existing leads. *Id.*

Additional standards are set out for dissemination of IPA data to foreign governments. The authorizing authority must ensure that arrangements are in place in the foreign country establishing requirements that correspond to the requirements discussed above, "to such extent (if any) as the [authorizing authority] considers appropriate," and, with respect to interception warrants, also for restrictions to be in place "to such extent (if any) as the [authorizing authority] considers appropriate" to prevent unauthorized disclosure. IPA §§ 54, 130, 151, 192. The Codes of Practice note that "[i]n most circumstances, intelligence sharing will take place with countries with which the United Kingdom has long and well established intelligence sharing relationships and which apply corresponding safeguards to material obtained under a warrant as

those provided in the Act. But there will also be occasions where material derived from [IPA] warrants may need to be shared with a country overseas with whom we do not have an existing intelligence sharing relationship and whose authorities do not apply safeguards to [IPA] material corresponding to those in the Act. Issuing authorities will need to consider the arrangements that should be in place to regulate such disclosure. These should require the person considering authorising such a disclosure to balance the risk that the material will not be subject to the same level of safeguards that it would be in this country, against the risks to national security if material is not shared." IoC CoP ¶ 9.28-9.29; EI CoP ¶ 9.35.

iii. Oversight

The UKIC's use of the IPA's investigatory powers is subject to independent oversight by the IPC and the Judicial Commissioners. The IPC is tasked with auditing, inspecting, and investigating the exercise of warrants under the IPA. IPA § 229.

The IPC and his team are responsible for continually inspecting the public authorities who use the investigatory powers. IPCO conducts its inspections on a proactive rather than reactive basis. As described in the UK Report and explained on IPCO's website,[12] IPCO conducts at least one inspection of the UKIC on each of the powers in a year (this includes the IPA as well as investigative powers authorized by RIPA 2000, which provides for the authorization of covert human intelligence sources and other covert surveillance techniques) as well as cross-cutting safeguards inspections. Nearly all of these are multi-day inspections. The inspections are conducted by teams of specialist inspectors accompanied by a Judicial Commissioner. Inspections are carried out to ensure that when investigatory powers are used, authorizations given are compliant with law; Codes of Practice requirements have been adhered to; and standards of good practice are maintained. Inspection teams review documentation, interview relevant staff members, and scrutinize records of the authority's use of an investigatory power. Inspectors will also review a variety of supporting documents such as risk assessments for covert human intelligence sources or policy logs, training modules and governance structures, and samples of material obtained through IPA warrants.

The IPC has access to the information needed to carry out its mandate. The IPA gives the IPC expansive powers to investigate and demand documents and other information from government personnel authorized to collect that information. IPA § 235. These powers include the Commissioner's authority to "carry out such investigations, inspections and audits as the Commissioner considers appropriate for the purposes of the Commissioner's functions." *Id.* Furthermore, the IPA requires public officials to "disclose or provide to a Judicial Commissioner all such documents or information as the Commissioner may require for the purposes of the Commissioner's functions." *Id.*

UKIC agencies are required to report compliance errors to the IPC. Specifically, UKIC agencies are required to report to the IPC any error of which they are aware in complying with any requirement imposed on it by the IPA or any other statute and which are subject to review by a Judicial Commissioner, and any error of a description "identified for this purpose in a code of

[12] IPCO, "Inspections", https://www.ipco.org.uk/what-we-do/inspections/ .

practice under Schedule 7." IPA §§ 235(6), 231(9). The Codes of Practice provide detailed guidance on error identification and what information should be reported to the IPC; any error should be reported within ten working days. IoC CoP ¶¶ 10.9-10.26; EI CoP ¶¶ 10.12-10.27. Further detailed guidance is provided on what records should be maintained to demonstrate compliance with the IPA and with the requirements of warrants, including a general requirement to maintain records for at least three years. IoC CoP ¶¶ 10.1-10.8; EI CoP ¶¶ 10.1-10.11.

If a compliance concern is identified either during an inspection or in normal business, IPCO may carry out additional *ad hoc* inspections in addition to scheduled inspections. If a compliance error that had not been reported is discovered, it does not appear that the IPC has explicit authority under the IPA to order that the UKIC agency take remedial measures. However as noted above there is a robust regime of mandatory compliance error reporting, and the UK advises that given the Judicial Commissioner's dual role in approving warrants and overseeing compliance, recommendations from Commissioners for remedial action are as a rule adopted. The IPCO website refers to the identification during its inspections of areas of non-compliance "that require addressing" and how to prioritize them for remedial action.[13] The Codes of Practice advise that when reporting errors to the IPC, a UKIC agency should report "the cause of the error; the amount of intercepted content or secondary data obtained or disclosed; any unintended collateral intrusion; *any analysis or action taken; whether the content or data has been retained or destroyed*; *and a summary of the steps taken to prevent recurrence*." IoC CoP ¶ 10.20; EI CoP ¶¶ 10.22 (emphasis added).

The IPA requires that the IPC make a yearly report to the Prime Minister, which must include "statistics on the use of the investigatory powers which are subject to review by the … Commissioner (including the number of warrants or authorizations issued, given, considered or approved during the year)," as well as information about "the number of relevant errors of which the … Commissioner has become aware during the year"; the number of errors determined to be "serious"; and the number of persons (targets) notified about the errors relating to them. *Id.* §§ 234, 231(8). The Prime Minister must make the report public, unless there is a statutory basis (*e.g.*, national security, economic well-being of the United Kingdom, etc.) to exclude certain provisions from publication. 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.[14]

The IPA oversight requirements are supported within UKIC agencies by rigorous training and technical requirements and centralized compliance programs. According to the UK Report, these include vetting of personnel, additional handling restrictions based on the classification of data, firewalling of internal networks, and access restrictions based on the established principle of "need to know." Additionally, for example, at GCHQ all staff and contractors must complete mandatory mission legalities training, and 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 organization. All training must be recertified at

[13] *See, e.g.*, IPCO, "Inspection Reports", https://www.ipco.org.uk/what-we-do/inspections/inspection-reports ("Areas of non-compliance identified during IPCO inspections indicate issues with the relevant law or Code of Practice that require addressing. They are graded to help a public authority prioritise what actions should be addressed most urgently").

[14] IPCO, "Annual Reports", https://www.ipco.org.uk/publications/annual-reports .

regular intervals. Technical controls prevent staff from requesting or accessing operational data unless they have completed the necessary training. GCHQ compliance officers are embedded within mission and technical teams and monitored by GCHQ's central compliance program.

iv. Individualized redress

A U.S. person concerned that his or her personal information that has been transferred to the United Kingdom has been access or handled unlawfully by a UKIC agency may submit a complaint to the Investigatory Powers Tribunal ("IPT"). The IPT is an independent UK court that decides complaints about, among other things, the conduct of UKIC agencies relating to surveillance, including allegations of violations of the IPA. The Tribunal has been operating for over twenty years, having been established in 2000 in the RIPA statute to replace several previous tribunals dating to 1985 that provided judicial redress in response to individuals' complaints alleging violations of surveillance laws.

The IPT provides a right of redress for anyone (regardless of citizenship) alleging violations of law by a UKIC agency "which he believes to have taken place in relation to him, . . . to any communications sent by or to him, or intended for him, or to his use of any . . . telecommunications service or telecommunication system" and relating to the IPA surveillance authorizations and related privacy safeguards discussed above. RIPA § 65(4). A complaint need not demonstrate that the complainant's personal data has in fact been accessed by a UKIC agency, but a complaint about secret intelligence surveillance must make a limited threshold showing that the complainant was at risk of being affected by the surveillance. An "individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or legislation permitting secret measures only if he is able to show that due to his personal situation, he is potentially at risk of being subjected to such measures."[15]

The IPT currently has fifteen members and operates independently. A person may not be appointed to the Tribunal unless he or she holds or has held a high judicial office, has been a member of the Judicial Committee of the Privy Council, satisfies judicial-appointment eligibility conditions on a seven-year basis, or is 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. RIPA sched. 3 § 1(1). Tribunal members are appointed for five-year periods, hold office during good behavior, and are eligible for reappointment. *Id.* §§ 1(2)-(3). They can be removed from office by the King, based on an address to the King presented by both Houses of Parliament or on a resolution of the Scottish Parliament after consideration by each House of Parliament and presentation to the King. *Id.* §§ 1(5)-(6). (Further grounds for removal are not specified.)

Like the independent redress functions of the Office of the Director of National Intelligence Civil Liberties Protection Officer ("ODNI CLPO") and Data Protection Review Court established under EO 14086, the IPT has the access to sensitive intelligence materials necessary to review individuals' complaints. Public officials are required "to disclose or provide

[15] Human Rights Watch Inc and Others v. the Secretary of State for the Foreign and Commonwealth Office and Others ([2016] UKIPTrib15_165-CH), judgment dated 16 May 2016, ¶ 19, reported in [2016] 5 WLUK 352.

to the Tribunal all such documents and information as the Tribunal may require for the purpose" of exercising its jurisdiction and powers. RIPA § 68(6)-(7). The Tribunal also may require the IPC or any Judicial Commissioner to provide assistance and to furnish the Tribunal with all documents and information as the Tribunal may require for the investigation of a matter or for its determination of a case before it. *Id.* § 68(2). The Tribunal's rules specify that it may receive evidence that may not be admissible in an ordinary court, IPT Rules § 13(1), which provides the IPT, according to the UK Report, greater freedom to review sensitive national security material relevant to the operations of UKIC agencies than the general UK courts.

Also similar to the ODNI CLPO and Data Protection Review Court established under EO 14086, the IPT has broad powers to make binding remedial orders. "On determining any proceedings, complaint or reference," the IPT "shall have power to make any such award of compensation or other order as they think fit." RIPA § 67(7). Example orders specified in the statute include orders to quash or cancel any warrant or authorization and orders to destroy records of information obtained under a warrant or authorization. *Id.*

The IPT like the ODNI CLPO and Data Protection Review Court must respect the secrecy requirements of intelligence operations and, as a result, the complainant may receive limited information about the review of a complaint. The IPT is required to ensure that information is not disclosed that may be "prejudicial to national security" or "the continued discharge of the functions of any of the intelligence services." IPT Rules 2018 § 7(1). Thus where the very fact of whether a complainant was subject to surveillance is secret, the IPT in its proceedings may not be able to disclose to the complainant any facts that it discovers relating to any surveillance that might have occurred, or whether a violation of law occurred, or whether the IPT decided to order any remedial action. The requirement in the IPT's rules to disclose its determinations, including any findings of fact, is made explicitly subject to this general requirement to protect sensitive intelligence information. *Id.* § 15(2), (3), (6).

Notwithstanding the requirement to respect the secrecy of intelligence operations, the IPT incorporates into its work, where possible, attributes of adversarial court proceedings, including innovative approaches to account for secrecy requirements. The IPT is not required to hold hearings in any case, and most of its cases are decided on the papers alone, but where possible and appropriate it does hold hearings either publicly or privately or in combination. The IPT's rules state that it "must endeavor," to the extent consistent with information security requirements, "to conduct proceedings, including any hearing, in public and in the presence of the complainant." IPT Rules § 10(4). The IPT website explains that one approach it takes in appropriate cases is to hold hearings on the basis of "assumed facts," so that without making factual findings the Tribunal "may be prepared to assume, for the sake of argument, that the facts the complainant asserts are true; then, acting upon that assumption, the Tribunal decides whether these asserted facts would constitute lawful or unlawful conduct. This has allowed the Tribunal to hold hearings in public with full adversarial argument as to whether the alleged conduct, if it had taken place, would have been lawful and proportionate."[16] The IPT publishes many of its

[16] IPT, "Open and Closed Hearings," at https://investigatorypowerstribunal.org.uk/open-and-closed-proceedings/ .

decisions[17] and has published several reports describing and providing statistical information on its operations and summarizing key decisions.[18]

The IPT may appoint at its discretion counsel to assist it in any case or circumstance it considers appropriate. IPT Rules § 12. The IPT may ask counsel to perform any function that would assist it, including to identify documents or parts of documents that may be disclosed to a complainant or made available to the general public; to cross-examine witnesses called by the respondent; or to ensure that all the relevant arguments on the facts and the law are placed before the IPT. *Id.* § 12(2). Where counsel is appointed, counsel must also seek to 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. *Id.* § 12(3). Unlike the special advocates appointed to assist the Data Protection Review Court pursuant to EO 14086, counsel that assist the IPT are not appointed in every case, might not be required (unless requested to do so by the IPT) to advocate regarding the complainant's interest in the matter, and do not ask questions of or otherwise communicate with the complainant.

v. Safeguards applicable to UKIC access to data in transit

The United States, the United Kingdom and other countries have consistently taken the position that access by the intelligence agencies of a destination country to data in transit between countries should not be a relevant consideration for the regulation of commercial flows of data.[19] The primary basis for this position is that a destination country's laws and practices regarding signals intelligence activities do not uniquely govern the privacy protection that is afforded to data located outside of that country or outside of any country. Rather, assessing possible privacy interferences with data while in transit would require reviewing the widely divergent laws and practices of many other countries than the destination country, and also the possibility of illicit access by a wide range of private actors. Accordingly, in determining whether the laws of the United Kingdom "require appropriate safeguards" for data "that is transferred from the United States to the territory of" the United Kingdom for purposes of section 3(f)(i)(A), it is reasonable to exclude from consideration whether UK laws require appropriate safeguards for signals intelligence activities not conducted in the territory of the United Kingdom.

For these reasons, the above analysis of UK laws has focused on the domestic signals intelligence activities of the UKIC, conducted within the territory of the United Kingdom. Nevertheless, for purposes of completeness and demonstrating the United Kingdom's overall commitment to privacy in this area, we review briefly here the privacy safeguards in UK law for extraterritorial signals intelligence activities. The IPA warrant regime itself may be used, and in some cases must be used, to authorize UKIC access to data located outside the United Kingdom. For example, the IPA authorizes serving a bulk interception warrant on a person outside of the

[17] IPT, "Judgments," at https://investigatorypowerstribunal.org.uk/judgments/ .
[18] IPT, "Reports," at https://investigatorypowerstribunal.org.uk/reports/ (providing links to reports published in 2010, 2016, and 2021).
[19] *See, e.g.*, U.S. Government White Paper, *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after* Schrems II at 17-18 (2020), *available at* https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF .

United Kingdom for the purpose of requiring assistance in the form of conduct outside of the United Kingdom, and sets out "additional requirements" to be taken into account when a bulk interception warrant is to require the assistance of a telecommunications operator located outside the United Kingdom, calling for consultations with the operator before the warrant is issued. IPA §§ 139, 149. Separately, the IPA specifies that a UKIC agency conducting bulk equipment interference outside the United Kingdom must obtain a warrant if "there is a British Islands connection," which is defined to include a surveillance purpose of obtaining information about a person in the United Kingdom. *Id.* § 13.

More generally, UK law provides privacy safeguards that apply globally to all signals intelligence activities, just as the United States has done in Executive Order 14086 other U.S. law. Even where acquisition by a UKIC agency of U.S. persons' communications while in transit from the United States to the United Kingdom does not require an IPA warrant, for example because of a lack of a British Islands connection, other limitations and safeguards apply. These globally applicable safeguards, similar to extraterritorial data acquisition under EO 12333, do not generally impose a requirement for independent approvals. Under UK law, such data access would be subject to section 7 of the ISA, which is entitled "Authorisation of acts outside the British Islands." The limitations and safeguards established in section 7 include that the Secretary of State must be satisfied that the authorized intelligence activities are necessary for the proper discharge of a function of an intelligence service; that there are satisfactory arrangements in force to secure that authorized activities will not go beyond what is necessary for the proper discharge of a function of an intelligence service and their nature and likely consequences will be reasonable, having regard to the purposes for which they are carried out; and that there are satisfactory arrangements in force with respect to the disclosure of information obtained. ISA § 7(3). These overseas surveillance powers under the ISA are subject to IPC oversight. Additionally, the IPT's jurisdiction includes violations by the UKIC of the ISA, so that a U.S. person may seek redress from the IPT for a complaint alleging violations of that statute with respect to any UKIC access to his or her data, whether authorized by the IPA or the ISA, while it is in transit from the United States to the United Kingdom.

c. Assessment

The Attorney General must determine for purposes of section 3(f)(i)(A) of Executive Order 14086, in consultation with the Secretary of State, the Secretary of Commerce, and the Director of National Intelligence, whether the laws of the United Kingdom "require appropriate safeguards in the conduct of signals intelligence activities for United States persons' personal information that is transferred from the United States to the territory" of the United Kingdom. As discussed above, section 3(f)(i)(A) does not require that the laws of the United Kingdom afford identical or reciprocal safeguards to those afforded by the United States. Rather, the required safeguards must be "appropriate."

The above discussion shows that intelligence laws in the U.S. and United Kingdom are similar in many respects, although they differ in other respects. In both countries, domestic access by intelligence agencies to the content of individuals' electronic communications requires prior review and approval, at either an individual or programmatic level, by an independent judicial officer. Additionally, the laws of both countries impose restrictions on the handling of

data collected for intelligence purposes, establish rigorous oversight procedures, and provide individuals a path to independent and binding redress.

There are certain areas where the laws of the United States and the United Kingdom diverge, and in some areas UK law either authorizes more expansive surveillance than U.S. law or has less restrictive safeguards. For example, UK law states in broader terms than EO 14086 the objectives for which signals intelligence activities may be authorized. As another example, targeted "thematic" warrants under the IPA may, after they are approved by a Judicial Commissioner, be expanded to add additional persons as targets without further approval by a Judicial Commissioner. Furthermore, the United Kingdom unlike the United States authorizes bulk collection of data domestically for national security purposes. Retention and dissemination standards are also set out in only general terms in the governing UK law. However, the UK system for intelligence surveillance, considered holistically, includes comprehensive limitations and safeguards, demonstrating its strong commitment to privacy. The United Kingdom's domestic bulk collection authorities are subject to rigorous safeguards, including detailed statutory restrictions on the querying of data collected in bulk, stringent documentation requirements, and independent approvals and oversight. Unlike the United States, the United Kingdom requires its intelligence agencies to obtain a warrant for the retention and querying of bulk personal datasets obtained through other lawful means. In areas where the IPA statute sets out only general guidance, for example for retention and dissemination of data, the Codes of Practice, which are admissible in court, provide more detailed or quantitative standards. Finally, the individualized judicial redress provided by the Investigatory Powers Tribunal is to our knowledge unique among OECD countries in establishing a tribunal dedicated and equipped to undertake the review of complaints alleging violations of laws governing surveillance activities while endeavoring to conduct open hearings where possible, publishing its decisions, and incorporating other attributes of regular adversarial court proceedings.

Based on the above analysis, it is reasonable and within the Attorney General's discretion to conclude, in consultation with the Secretary of State, the Secretary of Commerce, and the Director of National Intelligence, that notwithstanding certain areas of divergence between the laws of the United States and the laws of the United Kingdom, the laws of the United Kingdom require appropriate safeguards for purposes of a section 3(f)(i)(A) determination.

III. Determination that the United Kingdom permits, or is anticipated to permit, commercial data transfers to the United States

The second determination to be made to designate the United Kingdom, pursuant to section 3(f)(i)(B) of Executive Order 14086, is that the United Kingdom permits, or is anticipated to permit, the transfer of personal information for commercial purposes between the territory of the United Kingdom and the territory of the United States.

On July 16, 2020, the Court of Justice of the European Union ("CJEU") issued its judgment in the "*Schrems II*" case. Case C-311/18, *Data Prot. Comm'r v. Facebook Ir. Ltd, Maximillian Schrems*, ECLI:EU:C:2020:559 (2020). That judgment invalidated the adequacy decision issued by the European Commission in 2016 which concluded that the United States provides safeguards for government access to data, including signals intelligence activities, that

are "essentially equivalent" to safeguards afforded in the EU. Pursuant to the arrangements for the United Kingdom's departure from the EU, the *Schrems II* judgment remains part of retained UK case law. With respect to the possibility of UK data exporters relying on other transfer instruments under UK law (in particular International Data Transfer Agreements), the *Schrems II* judgment may influence how UK data exporters evaluate whether U.S. law provides sufficient privacy protections in the conduct of signals intelligence activities to permit transfers of personal data to the United States. Accordingly, the *Schrems II* judgment is sufficient to place in doubt whether the United Kingdom currently meets the requirement of section 3(f)(i)(B) of Executive Order 14086.

The strengthened safeguards for signals intelligence activities in Executive Order 14086 were designed to address the concerns of the CJEU as set out in the *Schrems II* decision. Based on those strengthened safeguards, the European Commission on July 10, 2023 adopted an adequacy decision for the United States under the EU-U.S. Data Privacy Framework. The United Kingdom is likewise working towards granting a data bridge to the United States for the UK Extension to the EU-U.S. DPF, which will permit under UK law the transfer of personal information between the territory of the United Kingdom and the territory of the United States. An essential step for granting the data bridge is that the Attorney General designate the United Kingdom as a qualifying state to make the redress mechanism established by the Executive Order available to UK individuals.

Section 3(f)(i) of Executive Order 14086 authorizes designation either "effective immediately or on a date specified by the Attorney General . . . ." Further, section 3(f)(i)(B) authorizes designation if the country "permit[s], *or [is] anticipated to permit*, the transfer of personal information for commercial purposes . . . ." (emphasis added). As noted above, based on the enhanced safeguards set forth in Executive Order 14086, the United Kingdom is anticipated to grant a data bridge to the United States. There is accordingly a sufficient basis to determine, in light of the standard in section 3(f)(i)(B), and in consultation with the Secretary of State, the Secretary of Commerce, and the Director of National Intelligence, that the United Kingdom is anticipated to permit the transfer of personal information for commercial purposes between the territory of the United Kingdom and the territory of the United States, and, further, to make the designation of the United Kingdom on a contingent basis, so that it will come into effect as of the date of the entry into force of UK regulations implementing the data bridge for the UK Extension to the EU-U.S. DPF.

IV. Determination that designation of the United Kingdom would advance U.S. national interests

The third determination to be made to designate the United Kingdom, pursuant to section 3(f)(i)(C) of Executive Order 14086, is that the designation would advance the national interests of the United States. Designating the United Kingdom is an essential step in bringing into place the UK Extension to the EU-U.S. DPF, which will provide vital benefits to citizens and businesses in both the United States and the United Kingdom. The UK Extension to the EU-U.S. DPF will enable the continued flow of data that underpins the $1.8 trillion U.S.-UK economic relationship and will enable businesses of all sizes to compete in each other's markets. There are accordingly sufficient grounds to conclude, in consultation with the Secretary of State, the

Secretary of Commerce, and the Director of National Intelligence, that it is in the national interest to designate the United Kingdom as a qualifying state.

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.