SAFE AND FREE:
NATIONAL SECURITY SURVEILLANCE AND THE RULE OF LAW ACROSS DEMOCRATIC STATES

The University of Texas at Austin
Strauss CENTER
for International Security and Law

NATIONAL SECURITY SURVEILLANCE IN THE UNITED KINGDOM

Ian Leigh

ABOUT THE AUTHOR

Ian Leigh is Emeritus Professor of Law at Durham University specialising in public law and human rights. His books on national security law include In From the Cold: National Security and Parliamentary Democracy (Oxford University Press, 1994), with Laurence Lustgarten, Who's Watching the Spies: Establishing Intelligence Service Accountability (Potomac Books, 2005) with Hans Born and Loch Johnson, International Intelligence Cooperation and Accountability (Routledge, 2011, with Hans Born and Aidan Wills) and Intelligence Oversight in the Twenty-First Century (Routledge, 2018, with Njord Wegge). He is co-author of two policy reports on intelligence reform: Making Intelligence Accountable (Norwegian Parliament Printing House 2005) and Making International Intelligence Cooperation Accountable (Norwegian Parliament Printing House 2015) and has acted as a consultant to the OSCE Office of Democratic Institutions and Human Rights, the Council of Europe, the Venice Commission, and to the UNDP on security sector reform.

ACKNOWLEDGEMENTS

This project was supported by funds from the Robert Strauss Endowment at the University of Texas at Austin and by a charitable gift from Microsoft. Each paper in the Safe and Free series reflects the views of its author. Editorial direction for the series was provided by Adam Klein, Director of the Robert Strauss Center for International Security and Law at the University of Texas at Austin. We are grateful to Strauss Center staff members Ali Prince and Brittany Horton, and to associate editors Zachary Badore, Seth Greenwald, and Taylor Helmcamp, for their help in shepherding the Safe and Free series to publication.

CONTENTS

NOVEMBER 2023

INTRODUCTION

The legal environment governing national security surveillance in the United Kingdom has undergone profound change in the last decade. For a prolonged period, the developing technological capabilities of the security and intelligence agencies were shrouded in both secrecy and legal obscurity. The public controversy and subsequent legal challenges arising from the revelations of Edward Snowden were the catalyst for a series of disclosures belatedly setting the record straight. They prompted official admissions of previously unacknowledged capabilities and the enactment of a more comprehensive and transparent surveillance regime. That regime is now contained in the Investigatory Powers Act 2016, which governs the various techniques available to the agencies, together with the authorisation and oversight processes.

I. INSTITUTIONS

Operational Entities

In the UK, electronic surveillance for national security purposes is conducted by the three main intelligence and security agencies: the Security Service (MI5), the Secret Intelligence Service (MI6) and Government Communications Headquarters (GCHQ). Surveillance can be of domestic or overseas targets, although, as explained in Part 3 below, more stringent requirements apply to domestic surveillance. In addition, the police are permitted to conduct targeted domestic surveillance for national security purposes. The agencies' use of surveillance is governed in general terms by their individual statutory charters and more specifically by the Investigatory Powers Act 2016, which is the detailed statutory code on specific forms of surveillance (both targeted and in bulk).

GCHQ has two roles: signals intelligence and information assurance.[1] The former, which covers all types of signals interception (and disruption) and decryption, is relevant here:

> to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material.[2]

The Security Service is the UK's domestic security agency, with primary responsibility for counter-terrorism (which accounts for around 80% of its work in practice).[3] The Service's statutory aims are more closely defined than those of the other agencies. These aims are: the protection of national security, including (but not limited to) protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers, and "actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means" ('counter-subversion').[4] A looser approach applies to SIS and GCHQ—the Intelligence Services Act refers to "the interests of national security, with particular reference to the Defence and foreign policies of Her Majesty's Government".[5] More specifically, the functions of MI6 are "to obtain and provide information relating to the actions or intentions of persons outside the British Islands . . . [and] to perform other tasks relating to the actions or intentions of such persons".[6] "Other tasks" covers a range of actions from espionage to covert action.

It is important to bear in mind that none of the security and intelligence agencies has a direct law enforcement role. Hence, in cases in which the ultimate goal is prosecution, they liaise with the police (e.g., in terrorism or espionage investigations) or another agency (such as Customs and Excise, in relation to organised crime), which will carry out a criminal investigation and arrest.

The Security Service is the UK's domestic security agency, with primary responsibility for counter-terrorism (which accounts for around 80% of its work in practice).

Authorising Entities

Unlike many other countries in which judicial authorisation is required, in the UK the tradition, dating from the sixteenth century, was for interception of communications to be approved by the Secretary of State (i.e., a government minister) under warrant. Thus, surveillance by the services requires explicit ministerial approval by the responsible Secretary of State, i.e., the Home Secretary in the case of the Security Service and the Secretary of State for Foreign and Commonwealth Affairs for SIS and GCHQ. This process was significantly modified by the addition of judicial confirmation (the so-called "double lock" system) under the Investigatory Powers Act 2016. The double-lock system requires that warrants or notices for both targeted surveillance and bulk powers be authorised by the Secretary of State[7] and subsequently approved by a Judicial Commissioner.[8] Judicial Commissioners must hold or must have held a high judicial office.[9]

It is a longstanding principle that the intercept product itself is barred from criminal proceedings, remaining in the background of an investigation.[10] This has the

important consequence that the legality of such surveillance cannot be challenged directly or indirectly at trial.

Oversight Entities

Whereas the Secretary of State and the Judicial Commissioners act as an *ex ante* check on surveillance by the agencies, three bodies are responsible for *ex post* review. Primary responsibility for oversight of national security surveillance falls to the Investigatory Powers Commissioner. However, policy aspects can be reviewed by the parliamentary Intelligence and Security Committee and individual complaints can also be brought before the Investigatory Powers Tribunal.

The Investigatory Powers Act 2016 brought together in a single and more powerful judicial Commissioner's office the various oversight Commissioners established under earlier legislation (so abolishing the offices of the Interception Commissioner and Intelligence Services Commissioner). The Investigatory Powers Commissioner (IPC) must hold or must have held a high judicial office,[11] but the Commissioner's role is distinct from that of the Judicial Commissioners.[12] The Investigatory Powers Commissioner's role is to keep under review the targeted and bulk surveillance powers available to the intelligence services,[13] especially with regard to the operation of safeguards to protect privacy.[14] The IPC has around 50 staff and is assisted by a technical advisory panel.[15]

The IPC has own-initiative powers to conduct thematic reviews of capabilities and to investigate serious errors. The security and intelligence services are required to disclose or provide all the necessary documents and information for the purposes of the IPC's functions[16] and to give any assistance the IPC requires in accessing apparatus, systems or other facilities of the intelligence services when exercising oversight functions.[17] The IPC is required to report annually[18] or at any time requested by the Prime Minister[19] or when the Commissioner considers it appropriate.[20] The Prime Minister is obliged to publish the Commissioner's annual reports and to lay a copy before Parliament, together with a statement whether any matter has been excluded.[21] If material is excluded on permitted grounds,[22] the Prime Minister is required to consult with the Commissioner.[23]

The Intelligence Services Act 1994 created a statutory committee—the Intelligence and Security Committee (ISC)—drawn from members of both Houses of Parliament. Its mandate is to review the policy, finance and administration (but not the operations)[24] of the agencies. This includes reviewing surveillance policy and administration. In particular, the ISC receives details of and keeps under review the "list of operational purposes"[25] used by the agencies in relation to bulk untargeted surveillance.[26] The committee has power to refer matters to the IPC for investigation, inspection or audit.[27] In such cases the IPC retains discretion over whether to investigate but, importantly, when an investigation is held, the Prime Minister is obliged to share the report with the ISC. [28] The ISC reports directly to Parliament but must send its reports beforehand to the Prime Minister and exclude matters that the Prime Minister considers would be prejudicial to the agencies.[29]

A specialist body, the Investigatory Powers Tribunal (IPT), has been established to investigate public complaints against the agencies or allegations of illegal interception by them.[30] Members of the Tribunal must hold or have held high judicial office or be qualified lawyers of at least ten years' standing. Any person may bring a claim and the IPT must determine all claims brought before it, except those it considers to be vexatious or frivolous.[31] The IPT is specified as the only appropriate forum for proceedings against any of the intelligence services concerning alleged incompatibility with European Convention rights and for complaints by persons who allege to have been subject to the investigatory powers of the Regulation of Investigatory Powers Act.[32] The IPT has jurisdiction to investigate any complaint that a person's communications have been intercepted and, where interception has occurred, to

examine the authority for such interception. No distinctions are made based on the complainant's nationality. The IPT is required to follow the principles applicable by a court on an application for judicial review[33] and can require anyone involved in the authorisation and execution of an interception warrant to disclose or provide documents, information[34] and all such assistance as it thinks fit from a relevant Commissioner.[35] There is a right to appeal on a point of law to the Court of Appeal.[36]

The Tribunal's jurisdiction covers covert investigative techniques (of all public authorities) and complaints of human rights violations by the intelligence services. In practice, complaints against the security and intelligence agencies account for approximately a third of its workload, with just under 100 such cases in 2021.[37] The Tribunal is a mixed adjudicatory and investigatory body. Once a complaint is made within its jurisdiction it has a duty to investigate. All public authorities (including the intelligence and security services) must assist it by disclosing documents and information of all kinds, regardless of security classifications or operational sensitivity. Where sensitive operational material is involved, however, it is able to sit in closed hearings with the complainant excluded, assisted by Counsel to the Tribunal. In such cases the practice is to adopt a mix of open and closed hearings and, so far as possible consistent with its duty not to disclose material prejudicial to national security, to give the complainant a reasoned decision and to make findings of fact and a summary determination in an open judgment, if necessary alongside a fuller closed judgment.

> ***In recent years around 85% of all complaints have been found to be outside the IPT's jurisdiction or to be vexatious or frivolous, around 11% have resulted in no determination and some 4% have been upheld.***

In recent years around 85% of all complaints have been found to be outside the IPT's jurisdiction or to be vexatious or frivolous, around 11% have resulted in no determination[38] and some 4% have been upheld. These figures cover complaints against public authorities within the IPTs jurisdiction rather than the security and intelligence agencies specifically. That said, there have been a number of high-profile open judgments in which the IPT has found against the security and intelligence agencies.

The 2016 Act also connects the IPC's audit role and the complaints-based jurisdiction of the IPT. The IPC is under a duty to assist the IPT and to issue an opinion on relevant matters, thus allowing the Commissioner's expertise to be put at its service.[39] There is also a duty to inform a person affected by a serious error (i.e., one that has caused them significant prejudice or harm) in matters under the IPC's review when the Commissioner determines that this is in the public interest.[40] The person concerned must also be informed of their right to apply to the IPT and given sufficient details to enable them to do so.

II. OPERATIONAL CAPABILITIES AND PRIORITIES

Operational control of SIS and GCHQ is in the hands of the Chief and Director, respectively, who are appointed by the Foreign Secretary.[41] Their intelligence collection priorities are set through "tasking" approved at the ministerial level in the annual United Kingdom's National Requirements for Secret Intelligence".

Much of the publicly available information concerning contemporary national security surveillance derives either directly or indirectly from the Snowden disclosures. The disclosures have had a significant impact in the UK since a number concern the work of GCHQ and its collaboration with the NSA in bulk collection of communication data, and this alerted the public to the previously unimagined scale of the agencies' activities. Those alleged activities include, among other things, the services' direct access to fibre optic cables that carry much communications traffic (TEMPORA),[42] the ability to compel production of certain data from the servers of leading internet companies under joint programmes (PRISM),[43] and extensive computer network exploitation to implant malware (in particular to access Belgacom and Gemalto, a major producer of mobile phone SIM cards).[44] There followed a spate of official reviews[45] and test cases brought by privacy campaigners, resulting in the official acknowledgement of a number of previously obscure or secret information-gathering techniques employed by the agencies, particularly in relation to bulk data and equipment interference.

III. PROCESS FOR CONDUCTING SURVEILLANCE

UK law distinguishes between targeted and bulk surveillance and according to the location of the persons under surveillance (i.e., whether one of them is within the British Isles or whether all are overseas), but not according to their nationality.

Targeted Interception and Examination

The 2016 Investigatory Powers Act establishes the process for domestic authorisations to obtain communications data.[46] Under the Act, the heads of the three intelligence services and the Chief of Defence Intelligence may apply to the Secretary of State for an interception warrant.[47] Interception warrants fall into two main relevant categories: targeted interception warrants and targeted examination warrants. The latter authorize the examination of material relating to a person in Britain that has previously been collected under a bulk interception warrant (discussed further below).[48]

An interception warrant may relate to a particular person or organization, or to a single set of premises. The Act also permits thematic warrants by providing that, in the context of a single investigation or operation, a warrant can also cover a group of linked persons, more than one person or organization, or a set of premises.[49]

The Secretary of State may issue an interception warrant in the interests of national security, for the purpose of preventing or detecting serious crime, in the interests of the economic well-being of the United Kingdom (in circumstances relevant to the interests of national security) or for giving effect to the provisions of a mutual assistance agreement.[50] The Minister must personally consider the application and be satisfied that the interception is both necessary and proportionate to the grounds specified.[51] Following the Minister's approval, a Judicial Commissioner considers whether to approve the warrant (or notice), applying judicial review principles (i.e., applying the common law tests of illegality, procedural impropriety and irrationality) to the Secretary of State's conclusions with regard to the necessity and proportionality of the warrant[52] and having particular regard to privacy duties.[53] Where a Judicial Commissioner refuses to approve a warrant, written reasons must be given by the Commissioner and these may be reconsidered by the Investigatory Powers Commissioner at the request of the person authorising the warrant. The Investigatory Powers Commissioner's decision is final.[54]

> ***Warrants are valid for six months, and retention notices can require the retention of data for 12 months. In urgent cases a warrant can be issued for targeted interception and equipment interference, as well as for bulk interception and bulk datasets without prior approval from the Judicial Commissioner.***

Warrants are valid for six months,[55] and retention notices can require the retention of data for 12 months.[56] In urgent cases a warrant can be issued for targeted interception and equipment interference, as well as for bulk interception and bulk datasets without prior approval from the Judicial Commissioner.[57] In these cases, however, the Commissioner must be notified and can decide whether they approve the warrant or not within three working days after the date of issue. In cases of refusal to approve a warrant, the implementing authority must, "so far as is reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible".[58] The Commissioner may also decide whether to request the destruction of any material collected or may impose conditions on its use or retention.[59]

Untargeted "Bulk" Powers

"Bulk powers" is the UK authorities' preferred terminology for non-targeted data gathering and analysis (rather than the more contentious "mass surveillance"). "Bulk" signifies the large scale of the enterprise, while nonetheless distinguishing it from universal or indiscriminate intelligence-gathering. Overall, only a small

proportion of internet traffic is collected under these powers, smaller proportions still are searched by automated means and only very small proportions of those will ever be read by a human analyst.[60] A review in 2016 by the Independent Reviewer of Terrorism Legislation endorsed the operational case for the various bulk powers which were in included in the IPA 2016 and gave examples of their use in practice.[61]

Domestic Use

Domestic authorizations to obtain communications data are governed by Part 3 of the 2016 Act. This provides for "bulk acquisition",[62] i.e., an instruction to a telecommunications operator to retain communications data (or so-called metadata)[63] and disclose it to the intelligence services.[64]

Before exercising one of the "bulk" powers, the services must obtain a warrant authorized by the Secretary of State and approved by a Judicial Commissioner. The warrants must specify the operational purposes for which any communications data obtained may be selected for examination. The operational purposes provided for in the Act are: national security, national security and the purpose of preventing or detecting serious crime or national security and in the interests of the economic well-being of the United Kingdom.[65] The "operational purposes" approved by the Secretary of State for bulk interception must, however, be specified in greater detail than the general description "national security."[66] Moreover, the "operational purposes" approved by the Secretary of State are required to be shown at three-month intervals to the Intelligence and Security Committee.[67]

When bulk acquisition is used domestically the intelligence services may collect only communications metadata rather than the content of the communications.[68] Such metadata are defined broadly, however: under the law metadata could include the location of mobile and fixed-line phones from which calls are made or received, the location of computers used to access the internet, the identity of a subscriber to a telephone service or a detailed telephone bill, websites visited from a device, email contacts, map searches, GPS location and information about devices connected to a Wi-Fi network. Such data can, for example, be used by the agencies to identify members of a terrorist network in contact with a particular email address.[69]

Foreign Use

The techniques permitted for foreign surveillance are more intrusive and allow for the collection and access of content of communications rather than only metadata.[70] The Act allows bulk collection through "interception of overseas-related communications"[71] (i.e, sent or received by a person outside Britain) and through "obtaining secondary data from such communications."[72] The provisions governing ministerial approval of "operational purposes" described above go some way to meeting the criticism that the 2016 Act permits mass surveillance. However, the language used to describe these would still allow a high degree of generality in the authorization of bulk powers, and a number of the controls governing how analysts can query databases of collected data remain in the form of internal procedures rather than legal requirements.

Equipment Interference

Part V of the 2016 Act gives the agencies explicit powers to interfere with equipment (typically, computers and mobile devices).[73] "Interference" is not defined more precisely in the Act. Presumably this reticence is intentional and is partly intended to future-proof the power, since more detailed definitions covering computer hacking and the implanting of viruses were readily available on the statute book.[74] Equipment interference warrants are issued by the Secretary of State[75] and approved by a Judicial Commissioner.[76] If the Commissioner refuses to approve the warrant, the agency may ask the Investigatory Powers Commissioner to review the decision.[77]

Bulk equipment interference[78] is only permitted outside Britain.[79] It covers "hacking or the implantation of software into endpoint devices or network infrastructure to retrieve intelligence, but may also include, for example, copying data directly from a computer".[80] Presumably, though not explicitly acknowledged, the interference could also take the form of implanting malware in a cyber-attack.

IV. RELEVANT LAW

The United Kingdom does not have a written constitution. Historically, matters of defence and national security were dealt with under powers derived from the prerogative (the residue of non-statutory power enjoyed by Crown and recognised at common law). In relation to surveillance, the prerogative was treated as authority for ministerial warrants for mail-opening and telephone tapping up until the 1980s. In this and subsequent reforms the influence of the UK's treaty obligations under the European Convention on Human Rights (Article 8 of which protects the right to respect for private life, home and correspondence) has been highly instrumental. It was to comply with the requirement under Article 8 that interferences with the right by public authorities should be 'in accordance with law' that powers to intercept communications were put onto a statutory basis in 1985.[81] Domestic and European jurisprudence on Article 8 has also featured prominently in framing subsequent legislation, including both the Regulation of Investigatory Powers Act 2000 and Investigatory Powers Act 2016.

The main changes introduced by the 2016 Act were to place added protections for certain categories of communications onto a statutory footing and to move away from ministerial warrants by introducing judicial approval. In the wake of the Snowden disclosures, several previously unacknowledged practices which rested on strained interpretations of oblique legal provisions or administrative guidance have been given an explicit statutory basis.

Limitations

Various limitations for the protection of human rights apply to surveillance. Firstly, there are overriding general duties which have regard to the impact on privacy.[82] Additional statutory requirements also protect legally privileged material and journalistic material.[83] Special enhanced safeguards apply if the warrant relates to the communications of Members of Parliament—in these cases the authorisation of the Prime Minister and a Judicial Commissioner is required.[84] Political neutrality is ensured by requirements for the heads of all three agencies to ensure that the services do not take any steps to further the interests of any UK political party.[85] General limitations on use of the service's powers in the protection of economic wellbeing apply for the protection of trade unions in Britain: a targeted warrant cannot be considered "necessary" if the information that would be obtained relates to trade union activity.[86] Similarly, an intelligence agency is prevented from using a class BPD warrant (that is, a warrant to access a "bulk personal dataset") to access a dataset if a substantial proportion of the dataset consists of sensitive personal data, such as data related to racial or ethnic origin, political or religious beliefs, or physical or mental health.[87]

Political neutrality is ensured by requirements for the heads of all three agencies to ensure that the services do not take any steps to further the interests of any UK political party.

V. TRANSPARENCY

For much of the twentieth century, Britain's legendary culture of secrecy cloaked the agencies and their surveillance practices so that the public had virtually no access to information about them. The three main security and intelligence agencies were created secretly in the early twentieth century, without reference to Parliament, under prerogative powers. Official acknowledgement of their existence and the granting of statutory charters only came much later: to the Security Service (MI5) in 1989[88] and to the Secret Intelligence Service (SIS or MI6) and the Government Communications Headquarters (GCHQ) in 1994.[89]

Sensitivity about the disclosure of intelligence features prominently in the oversight arrangements. Although the ISC has power to send for persons and papers, in other respects its information-gathering powers are limited. The agency heads may refuse to disclose "sensitive information",[90] i.e., information that might lead to the identification of sources, other forms of assistance given to the agencies, or operational methods; information concerning past, present or future specific operations; or information provided by a foreign government which does not consent to its disclosure. Within these categories refusal is *discretionary*.

Equally, the complaints-handling procedures before the IPT are designed to protect the agencies and to prevent the complainant from using the proceedings to discover if they are lawfully under surveillance. At their conclusion, the IPT gives a simple statement either that it has found in favour of the complainant (i.e., that there has been unlawful action against him or her) or that "no determination has been made in his favour".[91] In the event of a successful claim, the IPT may award compensation and make such other orders as it thinks fit, including orders quashing or cancelling interception warrants and requiring the destruction of any records so obtained.[92] It must also submit a report to the Prime Minister.[93]

Despite the restrictions built into the statutory scheme,[94] in a series of careful judgments (mostly arising from the Snowden allegations) the IPT has dealt with some serious allegations (notwithstanding the agencies' policy to Neither Confirm Nor Deny them) by considering the relevant legal arguments on the basis of "hypothetical facts".[95] This allows the IPT to make a binding pronouncement of legal principle even where the claimant cannot realistically discharge the burden of proof.

> ***One result of the debate surrounding the Snowden disclosures has been a substantial increase in transparency. Some of the resulting legal challenges before the IPT forced the government into greater candour about the various surveillance techniques used by the agencies, GCHQ in particular.***

One result of the debate surrounding the Snowden disclosures has been a substantial increase in transparency. Some of the resulting legal challenges before the IPT forced the government into greater candour about the various surveillance techniques used by the agencies, GCHQ in particular. Examples include the disclosure of secret internal guidance on the searching by GCHQ of bulk data collected by the NSA[96] and the publication of a Draft Equipment Interference Code of Practice of computer network exploitation by GCHQ.[97] The reforms introduced by the 2016 Act amount to a detailed and comprehensive surveillance code establishing an explicit basis for and procedural safeguards governing a number of previously unacknowledged surveillance techniques. The annual reports of the Investigatory Powers Commissioner[98] provide a wealth of detail, in contrast to the brief and heavily redacted reports of the previous institutions. These include data on the numbers of authorisations and detailed accounts of the oversight activities (such as inspections) conducted in relation to each agency and the various types of surveillance.

Notwithstanding these developments, there remain considerable obstacles to obtaining insider information on the contemporary operation of national security surveillance. All disclosures by members or former members of the security and intelligence agencies are subject to draconian criminal penalties under the Official Secrets Act 1989.[99] There is no statutory public interest defence and the country's highest court rejected an attempt by a former MI5 officer to invoke a defence on these lines in 2002.[100] The extent of the prohibition is such that there is simply no safe route for unauthorised whistleblowing, even to the Intelligence

and Security Committee of Parliament or to the Commissioner's office.[101] Remarkably, under the 1989 Act even journalists can be become liable for damaging disclosures of information of this kind that has come into their possession.[102]

It is open to question, in the light of the developing jurisprudence of the European Court of Human Rights, whether the blanket nature of these restrictions would now withstand detailed human rights challenge. Notably, the Court has interpreted the right of freedom of expression and information to provide protection to a whistleblower seeking to expose illegal interception of communications by the Romanian Intelligence Service, emphasising that alternative mechanisms for raising concerns must be effective in practice.[103] Be that as it may, the practical consequence of the current position is that there is little unofficial information on the operation of the system which would add colour and context to the official accounts.

VI. REFORM

The Investigatory Powers Act 2016 brought the existing powers for the agencies and law enforcement bodies for surveillance of communications and access to communications data together in one place. It also significantly extended the powers to cover additional new technologies and to allow access to internet connection records. It gave comprehensive statutory underpinning for the first time to a variety of "untargeted" or "bulk surveillance" techniques used by the security and intelligence agencies, in particular, to bulk collection and examination, to analysis of bulk personal datasets and to equipment interference. These changes reflect a shift in intelligence techniques away from traditional interceptions of communications and towards the collection and analysis of communications data, designed to establish the movement and location of individuals, their habits (including internet browsing), their networks, contacts and travel.

Prior to the 2016 Act, a distinction applied between interception warrants (identifying specific targets for surveillance and approved individually) and "certificated warrants" (for external communications where the originator or recipient of the communication was outside the country). The latter, approved by the Foreign Secretary, needed only to specify general categories of information and were then subject to less rigorous controls over the examination of material obtained. Interception of metadata was likewise subject to lighter regulation and could be undertaken by a number of public agencies, after the approval of a magistrate. The legislation did not adequately distinguish between metadata and interception of the contents of communication in a way corresponding to current technology. Nor were there any effective safeguards against the transfer of intercepted material to overseas agencies such as the NSA or adequate controls over material flowing the other way.

The Snowden disclosures brought a number of privacy concerns to light. These included the treatment by the UK agencies of communications with overseas based internet platforms (such as Yahoo, Google and Facebook) as subject to the external regime. Moreover, the use of "thematic" interception warrants covering defined groups of individuals or networks, rather than identified individuals, was revealed in 2015.[104]

A review published in 2016 also revealed that under successive governments, the agencies had been engaged in the clandestine acquisition of bulk communications data.[105] That practice relied on an obscure power, originally intended for a different purpose, to give ministerial directions to communications providers on grounds of national security.[106] No attempt had been made to inform Parliament or to seek more explicit legal powers, either when a comprehensive review of the surveillance legislation was undertaken in 2000 or when the intelligence oversight scheme was reformed in 2013.

VII. CONCLUSION

The environment in which the security and intelligence agencies operate has undergone rapid change in the past quarter-century. Most dramatic of all, perhaps, has been the technological change over the period, with many of the capabilities of the agencies laid bare since 2013 by the unprecedented disclosures of Edward Snowden. The result was a long overdue public and parliamentary debate about surveillance, resulting in the Investigatory Powers Act 2016 and a detailed and comprehensive legal framework that regulates and gives legitimacy to the agencies' capabilities.

ENDNOTES

1 For the history of GCHQ, *see Our origins & WWI*, GCHQ, Our origins & WWI - GCHQ.GOV.UK (last visited 20 June 2022); J. Ferris, BEHIND THE ENIGMA; THE AUTHORISED HISTORY OF GCHQ (2021); R. Aldrich, GCHQ: THE UNCENSORED STORY OF BRITAIN'S MOST SECRET INTELLIGENCE AGENCY (2011).
2 Intelligence Services Act 1994, sec. 3(1)(a).
3 For historical accounts, *see* C. Andrew, SECRET SERVICE: THE MAKING OF THE BRITISH INTELLIGENCE COMMUNITY (1986), 121ff; C. Andrew, DEFENCE OF THE REALM: THE AUTHORIZED HISTORY OF MI5 (2009), sec. A, chs. 1–3.
4 Security Service Act 1989, sec. 1.
5 Intelligence Services Act 1994, secs. 1(2)(a), 3(2)(a). GCHQ's functions can also be exercised under sec. 3(2) "in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands"; and "in support of the prevention or detection of serious crime".
6 Intelligence Services Act 1994, sec. 1(1). On MI6, *see Secret Intelligence Service MI6*, SIS.gov.uk, http://www.mi6.gov.uk/output/sis-home-welcome.html (last visited 27 July 2023). An official history of the early decades of SIS was published in 2010. See K. Jeffery, MI6: THE HISTORY OF THE SECRET INTELLIGENCE SERVICE 1909–1949 (2010).
7 Investigatory Powers Act 2016 (hereafter "IPA"), secs. 19 (interception and examination), 87 (retention of communications data), 102 (equipment interference). "Secretary of State" is the generic legal term used for conferral of powers and duties on government ministers. Statutes do not usually specify which minister is legally responsible.
8 IPA, secs. 23 (interception and examination), 87(1)(b) (retention notices), 102(1)(d).
9 IPA, sec. 227(2).
10 IPA, sec. 20(5) (this section precludes authorising a warrant for the sole purpose of gathering evidence for use in legal proceedings).
11 IPA, sec. 227(2).
12 IPA, sec. 229(4).
13 IPA, sec. 229(1).
14 IPA, sec. 229(5).
15 IPA, secs. 246, 247.
16 IPA, sec. 235(2).
17 IPA, sec. 235(3)–(4).
18 IPA, sec. 234(1).
19 IPA, sec. 234(3).
20 IPA, sec. 234(4).
21 IPA, sec. 234(6).
22 IPA, sec. 234(7).
23 IPA, sec. 234(7).
24 Subject to limited exceptions.
25 IPA, sec. 142(4).
26 The Secretary of State is required to send the list to the ISC at 3-monthly intervals. IPA, sec. 142(8). The Prime Minister must review the list at least annually. IPA, sec. 142(10).
27 IPA, sec. 236.
28 IPA, sec. 234.
29 Justice and Security Act 2013, sec. 3.
30 Regulation of Investigatory Powers Act 2000 (hereafter "RIPA"), sec. 65.
31 RIPA, sec. 67(1), (4), (5).
32 RIPA, sec. 65(2).
33 RIPA, sec. 67(2), (3)(c).
34 RIPA, sec. 68(6)–(7).
35 RIPA, sec. 68(2).
36 IPA, sec. 242.
37 The details in this paragraph are taken from: Investigatory Powers Tribunal, *Report 2016–2021*, IPT Report (2022), https://investigatorypowerstribunal.org.uk/wp-content/uploads/2023/03/Report-of-the-Investigatory-Powers-Tribunal-2016-2021.pdf.
38 The details in this paragraph are taken from: Investigatory Powers Tribunal, Report 2016–2021, IPT Report (2022), https://

investigatorypowerstribunal.org.uk/wp-content/uploads/2023/03/Report-of-the-Investigatory-Powers-Tribunal-2016-2021.pdf.

39 IPA, sec. 232.

40 IPA, sec. 231.

41 Intelligence Services Act, secs. 2, 4.

42 TEMPORA involved the interception by GCHQ of digital traffic flowing through the underwater fibre optic cables landing in the UK.

43 "The PRISM programme involved the collection by the NSA of data from the servers of nine US internet companies (Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple—"*the Prism Providers*"). Types of data collected included a range of digital information such as email, chat, videos, photos, stored data, VOIP, video conferencing and online social networking details." (Anderson, *A Question of Trust*, Annex 7).

44 *Id.* at Annex 7.7.

45 *Privacy and Security: A Modern and Transparent Legal Framework*, Intel. & Sec. Committee Parl. (March 2015), HC 1075, https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf (hereafter "*Privacy and Security*"); David Anderson Q.C., *A Question of Trust: Report of the Investigatory Powers Review* (June 2015), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/434399/IPR-Report-Web-Accessible1.pdf (hereafter "*A Question of Trust*"); Panel of the Independent Surveillance Review, *A Democratic Licence to Operate: Report of the Independent Surveillance Review*, Royal United Servs. Inst. (July 2015), https://rusi.org/explore-our-research/publications/whitehall-reports/a-democratic-licence-to-operate-report-of-the-independent-surveillance-review.

46 IPA, part 2, ch.1.

47 IPA, sec. 30.

48 A targeted examination warrant is required whenever a member of an intelligence service wishes to look at material which relates to a person who is known to be in the British Islands and when he or she believes that it is necessary and proportionate to select the content of that person's communications for examination. IPA, sec. 15(3).

49 IPA, sec. 17(2). A warrant may also relate to testing or training activities. IPA, sec. 17(3).

50 IPA, sec. 20(2). "Economic wellbeing" is not defined, although subsection (4) makes clear that a warrant may only be considered necessary in the interests of the economic well-being of the UK when it relates to the acts or intentions of persons outside the British Islands.

51 A warrant cannot be considered necessary if its only purpose is gathering evidence for use in legal proceedings, or only on the basis that the information that would be obtained relates to trade union activity in the British Islands. IPA, sec. 20(5)–(6).

52 IPA, sec. 23(1).

53 *See* IPA, sec. 2.

54 IPA, sec. 23(4)–(5).

55 IPA, secs. 32(2)(b) (interception and examination), 116(2)(b) (equipment interference).

56 IPA, sec. 87(3). Retention notices must be approved by the Secretary of State (IPA, sec 88) and reviewed by a Judicial Commissioner (IPA, sec. 89).

57 IPA, secs. 24, 109 (targeted interception and examination and equipment interference warrants, respectively). IPA, secs. 180 (bulk equipment interference), 209 (bulk personal datasets).

58 IPA, secs. 25 (2), 110(2), 181(2), 210(2).

59 IPA, sec. 25(3).

60 *Privacy and Security* at 31–32 (discussing GCHQ practice).

61 David Anderson Q.C., *Report of the Bulk Powers Review*, OGL Report (Aug. 2016), Cm. 9326, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf.

62 Privacy International challenged the bulk acquisition powers under section 94 of the Telecommunications Act 1984 before the Investigatory Powers Tribunal. The IPT ruled that until 4 November 2015, when stricter safeguards were introduced, the intelligence services were violating the right to private life (Article 8 of the ECHR). *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs* [2016], UKIP Trib. 15_110-CH, 17 Oct. 2016.

63 Communications data refers to the "who," "when," "where," and "how" of a communication, but not its content.: IPA, secs. 261, 262.

64 IPA, secs 158–175.

65 IPA, secs. 138 (bulk interception), 158 (bulk acquisition), 178 (bulk equipment interference), 204–205 (bulk personal datasets).

66 IPA, secs. 142 (bulk interception), 161 (bulk acquisition), 183 (bulk equipment interference), 212 (bulk personal datasets).

67 IPA, secs. 142 (bulk interception), 161 (bulk acquisition), 183 (bulk equipment interference), 212 (bulk personal datasets).

68 IPA, sec. 158(6).

69 *A Question of Trust* at 159.

70 IPA, part 6, ch. 1.

71 IPA, sec. 136(2)(a).

72 IPA, sec. 136(2)(b).

73 Previously, the agencies relied on less specific powers to interfere with property under section 5 of the Intelligence Services Act 1994 (and related statutory Codes of Practice) to carry out Computer Network Exploitation. *Privacy International and Greenmet &*

Others v. (1) The Secretary of State for Foreign and Commonwealth Affairs (2) The Government Communications Headquarters, IPT 14/85/CH 14/120-126/CH.

74 *See* Computer Misuse Act 1990.

75 IPA, sec. 102. A warrant can only be issued if it is necessary in the interests of national security, for the purpose of preventing or detecting serious crime, or in the interests of the economic wellbeing of the United Kingdom (so far as those interests are also relevant to the interests of national security), and proportionate to the intended outcome. IPA, sec. 102(5).

76 IPA, sec. 108.

77 IPA, sec. 108(5).

78 IPA, part 7.

79 IPA, sec. 176(1)(c). Prior to the entry into force of the 2016 Act, bulk powers interference had never been used in the United Kingdom. *A Question of Trust* at 184.

80 *Id.* at 34.

81 Interception of Communications Act 1985, following the judgment of the European Court of Human Rights in *Malone v. UK* (1985), 7 EHRR 245.

82 IPA, sec. 2.

83 IPA, secs. 27–29.

84 IPA, sec. 26.

85 Security Service Act 1989, sec. 2; Intelligence Services Act 1994, secs. 2, 4.

86 IPA, sec. 20(6).

87 IPA, sec. 202(1); Data Protection Act 1998, sec. 2(a)–(f).

88 Security Service Act 1989.

89 Intelligence Services Act 1994.

90 Justice and Security Act 2013, sched. 1.

91 Regulation of Investigatory Powers Act 2000, sec. 68(4).

92 Regulation of Investigatory Powers Act 2000, sec. 67(7).

93 Regulation of Investigatory Powers Act 2000, sec. 68(5).

94 The procedure has been found to be compatible with the right to fair trial (Article 6) of the ECHR. *Kennedy v. UK* (2011), 52 EHRR 4.

95 E.g., *Liberty and others v. The Secretary of State for Foreign and Commonwealth Affairs and others*, Case Nos. IPT/13/77/CH; 13/92/CH; 13/194/C and 13/204/CH, [2015] UKIP Trib. 13_77 –H. (available at https://www.ipt-uk.com/judgments.asp).

96 *Liberty and others v. The Secretary of State for Foreign and Commonwealth Affairs and others*, Case Nos. IPT/13/77/CH; 13/92/CH; 13/194/C and 13/204/CH, [2015] UKIP Trib 13_77 –H at 153-154. (available at https://www.ipt-uk.com/judgments.asp).

97 Following *Privacy International and Greenmet & Others v. (1) The Secretary of State for Foreign and Commonwealth Affairs (2) The Government Communications Headquarters*, IPT 14/85/CH 14/120-126/CH. (available at https://www.ipt-uk.com/judgments.asp).

98 The annual reports can be accessed at: https://www.ipco.org.uk/publications/annual-reports/.

99 Official Secrets Act 1989, sec. 1(1). The provision also applies to other "notified" persons, such as government officials who work closely with the agencies. Additionally, section 4 imposes liability for disclosures without lawful authority concerning national security surveillance.

100 *R v. Shayler* [2002], UK HL 11.

101 For detailed analysis, *see* Ashley Savage, LEAKS, WHISTLEBLOWING AND THE PUBLIC INTEREST: THE LAW OF UNAUTHORIZED DISCLOSURES (2016), ch 6.

102 Official Secrets Act 1989, sec. 5.

103 *Bucur and Toma v. Romania*, App. no. 40238/02 (ECHR, 8 Jan. 2013).

104 *Privacy and Security* at paras. 42ff. Section 7(2) of the IPA now provides explicitly that, in the context of a single investigation or operation, a warrant can also cover a group of linked persons, to more than one person or organisation or set of premises.

105 Interception of Communications Commissioner, *Review of the Directions given under section 94 of the Telecommunications Act (1984)*, Gov.UK Corporate Report (July 2016), HC 33, https://www.gov.uk/government/publications/review-of-directions-given-under-section-94-of-the-telecommunications-act-1984. *See* Rt. Hon. Theresa May MP, H.C. Deb. (4 Nov. 2015), col. 971 (statement to Parliament by the Prime Minister in November 2015).

106 Telecommunications Act 1984, sec. 94.