The Human Rights, Big Data and Technology Project

Regulation of Big Data Surveillance by Police and Intelligence Agencies

by

Carly Nyst

E·S·R·C ECONOMIC & SOCIAL RESEARCH COUNCIL

Human Rights Centre | University of Essex

1. Background

Recent years have seen the emergence of a new era of police and intelligence surveillance, once which seeks to exploit the massive growth in accessible personal data as a result of the digitisation of communications and information. Previously, surveillance techniques such as human intelligence, wire-tapping, mail interception and covert physical and video surveillance were the primary tools by which intelligence was acquired by police and security services. Yet today those same agencies have pivoted to an intelligence posture which prioritises and preferences "big data", as evidenced by the establishment, in late 2015, by the CIA of its first new Directorate in 50 years – the Directorate for Digital Innovation. Governments are investing in technologies and adopting regulation to enable the acquisition and use of massive digital data sets to ascertain relationships, create profiles and understand behaviour. As the US National Security Agency boldly declared in an internal document, made public by whistleblower Edward Snowden, agencies have entered a "golden age" of digital surveillance.[1]

As a prelude to further study in this field, the Human Rights, Big Data and Technology Project seeks to undertake a mapping of laws and regulations pertaining to "big data surveillance" by police and intelligence agencies in five countries: the UK, USA, Germany, Brazil and India. This is not an exhaustive study of surveillance law in the respective countries, but rather zeros in on surveillance laws which pertain to the acquisition of "big data". For the purposes of this study, we have defined "big data surveillance" as the *monitoring, interception or acquisition of digital data in bulk or untargeted manner*.

2. Introduction to Big Data Surveillance in the United Kingdom

In November 2016, after more than a year of parliamentary and public debate, the Investigatory Powers Act 2016 ("the IP Act") became law. The IP Act replaces Part I, Chapter I of the Regulation of Investigatory Powers Act 2000 ("RIPA") and the emergency legislation passed in July 2014, the Data Retention and Investigatory Powers Act ("DRIPA"). It also replicates and

[1] NSA sigint strategy 2012-2016. The original document describes the current day as "the golden age of Sigint", using the colloquial term to refer to signals intelligence, the monitoring and interception of radio and radar signals.

extends powers contained in Part I, Chapter II of RIPA, the Wireless Telegraphy Act 2006, the Intelligence Services Act 1994, the Police Act 1997, the Security Service Act 1989 and the Telecommunications Act 1984, and introduces new powers.

The IP Act is possibly one of the detailed surveillance laws in the world, particularly with respect to provisions pertaining to the intelligence and security services, and is comparatively technologically advanced. It authorises big data surveillance in five forms:

- Bulk interception of communications content: Part 6, Chapter 1 sanctions the interception of overseas-related communications and communications data in bulk by intelligence agencies;
- Bulk equipment interference: Park 6, Chapter 3 sanctions the interference with equipment for the purpose of obtaining communications and equipment data;
- Retention of communications data: Part 4 of the Act empowers the Secretary of State to require telecommunications operators to retain communications data, including "internet connection records" in bulk for up to twelve months, while Part 3 envisages the imposition of digital "filtering arrangements" to facilitate immediate targeted access to such data by both police and intelligence agencies;
- Bulk access to communications data: Part 6, Chapter 2 enables the Secretary of State to issue a bulk acquisition warrant permitting the bulk acquisition of communications data by intelligence agencies;
- Bulk access to other personal datasets: Part 7 permits intelligence agencies to seek the retention of either a class of, or specific, "bulk personal datasets", the nature of which is such that the majority of individuals to whom the dataset pertains are not, and are unlikely to become, of interest to the intelligence services in the exercise of their functions.

Each of these powers is exercisable in the interests of national security, for the prevention and detection of serious crime, and in the interests of the economic well-being of the United Kingdom so far as those interests are relevant to the interest of national security. For the purpose of the Act, "serious crime" in a crime where:

- the offence is an offence for which a person who has reached the age of 18 (or, in relation

to Scotland or Northern Ireland, 21) and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more, or

- the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose.

In addition to the powers contained in the IP Act, British police and intelligence agencies exercise some capabilities, under the broad ambit of the directed surveillance provisions of Part II of RIPA, could be described as big data surveillance. These include both Open Source Intelligence ("OSINT") and Social Media Intelligence ("SOCMINT") in monitoring online. behaviour.

Likewise, there are other powers would could be exercised under the Intelligence Services Act 1994, such as the deployment of Computer Network Operations, or Computer Network Attacks, which inevitably collects large amounts of information about the networks they are attacking.

Generally speaking, the exercise of big data surveillance methods in the United Kingdom is not subject to prior judicial authorisation; although the Investigatory Powers Act requires a Judicial Commissioner review the Secretary of State's authorisations in certain circumstances using judicial review principles, which fall slightly short of requiring a full merits review of the original warrant application. There is no requirement in any British legislation pertaining to surveillance that an authorising entity consider or verify the existence of a reasonable suspicion against any person prior to approving or authorizing the surveillance measure, instead the test of necessity and proportionality is applied.

As a result of the Investigatory Powers Act, the surveillance oversight regime is currently undergoing fundamental changes. The IP Act established an Investigatory Powers Commissioner with oversight over the interception of communications and the acquisition and retention of data. The Commissioner's office will take on the functions of the existing Interception of Communications Commissioner, the Chief Surveillance Commissioner and the Intelligence Services Commissioner. The practical amalgamation of those offices is ongoing.

In addition to the Investigatory Powers Commissioner, two other oversight mechanisms will continue to operate: the Intelligence and Security Committee of Parliament, which provides parliamentary oversight over the activities of the intelligence and security agencies, and the Investigatory Powers Tribunal, which has jurisdiction over all complaints regarding interception of communications, and all matters pertaining to the intelligence services. Because there is no obligation under British law for police or intelligence agencies to notify individuals that they have been subject to surveillance, the standing requirements applicable to an application before the Investigatory Powers Tribunal are comparatively low.

Finally, with respect to the application of data protection law to big data surveillance, the Data Protection Act 1998 is subject to exemptions for the safeguarding of national security, which are applied on a case by case basis. In addition, the Secretary of State can, in accordance with Section 28 (1) of the Act, certify the exemption of certain authorities from particular parts of the Act. The Secretary of State has indeed issued such certificates exempting GCHQ, MI6 and MI5 from the data protection principles, as well as provisions regarding subject access. Section 29 of the Act pertains to exemptions for processing related to the prevention and detection of crime, which are somewhat more circumscribed than those pertaining to national security.

3. Interception

Bulk Interception

Although the UK is the only country to deploy the term “bulk interception” in its surveillance legislation, the practice that the term refers to is engaged in by a number of countries, often outside of regulatory frameworks. Manufacturers of bulk interception technology often refer to “passive monitoring” or “fibre optic cable interception”, while in Germany the term “strategic monitoring” is utilised. Indeed, “bulk interception” has only recently been introduced into the British regulatory lexicon, too; it was first officially utilised to refer to the non-targeted interception of communications permitted under section 8(4) of RIPA by the Intelligence and Security Committee in its March 2015 report, *Privacy and Security: A modern and transparent legal framework.* That report called for a new, more transparent legal framework to govern interception

and surveillance by the intelligence and security services. The IP Act was enacted less than two years later, and Part 6, Chapter 1 of that Act provides for bulk interception warrants.

The Draft Interception Code of Conduct, released in February 2017, describes bulk interception as "a strategic intelligence gathering capability, whereas targeted interception is primarily an investigative tool that is used once a particular subject for interception has been identified."[2] Bulk interception warrants do not need to be targeted towards particular individuals or limited in any way by the number of communications affected.

The thrust of the bulk interception regime is the interception of "overseas-related" communications outside of Britain: bulk interception warrants must have their purpose the interception of communications sent or received by persons outside the United Kingdom. In practice, however, given the global nature of communications, this restriction does not meaningfully limit the interception of British persons' communications.

The bulk interception regime provides for a single warrant to be issued which covers both the interception of communications content and "secondary data", and the subsequent selection of that content and data for examination. There is no need to apply for a secondary warrant for examination unless relevant content will be examined in breach of a prohibition elaborated in section 152, which prohibits the selection for examination of material for the purpose of identifying communications of individuals known to be in the British Islands.

Bulk interception warrants clearly permit big data surveillance. According to the Draft Interception Code of Conduct, it is envisaged that bulk interception will be used to, for example,

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

[2] Interception Code of Conduct February 2017 Draft, para. 6.7.

to the United Kingdom.[3]

Requirements for authorisation

Under the IP Act, the Secretary of State may issue a bulk interception warrant upon the application of the intelligence services under certain conditions.[4] A bulk interception warrant is defined as a warrant which:

- Has as its main purpose the interception of overseas-related communications and the obtaining of secondary data from such communications, where "overseas-related" refers to communications sent or received by persons outside the British Islands;[5] and
- Authorises the relevant person to secure the interception of communications, obtain secondary data, select for examination intercepted content or data, and disclose anything obtained under the warrant to authorised persons.[6]

The Secretary of State may issue a warrant where the following conditions are met:

- The warrant contains a provision stating that it is a bulk interception warrant,[7] and is addressed to the head of the intelligence service by whom, or on whose behalf, the application is made;[8]
- The warrant is necessary either
    - in the interests of **national security**,[9] provided it is not necessary only for the purpose of gathering evidence for use in any legal proceedings;[10]
    - for the purpose of **preventing and detecting serious crime**,[11] provided it is not necessary only for the purpose of gathering evidence for use in any legal proceedings;[12]
    - in the interests of the **economic well-being of the United Kingdom** so far as those interests are relevant to the interest of national security[13] provided that the

[3] Interception Code of Conduct February 2017 Draft, para. 6.3.
[4] Section 138, Investigatory Powers Act 2016
[5] Section 136 (2) and (3), Investigatory Powers Act 2016
[6] Section 136 (4), Investigatory Powers Act 2016
[7] Section 142(1), Investigatory Powers Act 2016
[8] Section 142(2), Investigatory Powers Act 2016
[9] Section 138 (1)(b)(i), Investigatory Powers Act 2016
[10] Section 138(4), Investigatory Powers Act 2016
[11] Section 138(2)(a), Investigatory Powers Act 2016
[12] Section 138(4), Investigatory Powers Act 2016

information which it is considered necessary to obtain is information relating to the acts or intentions of persons outside the British Islands,[14] and provided it is not necessary only for the purpose of gathering evidence for use in any legal proceedings.[15]

- The conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.[16] In considering whether a bulk interception warrant is necessary and proportionate, the Secretary of State must take into account whether what is sought to be achieved by the warrant could reasonably be achieved by other less intrusive means;[17] and
- The warrant specifies the operational purposes for which any intercepted content or secondary data obtained under the warrant may be selected for examination,[18] and the Secretary of State is satisfied that each of the specified operational purposes is a purpose for which the examination may be necessary.[19] The operational purposes must be ones specified in a list maintained by the heads of the intelligence services as acceptable operational purposes,[20] and in the warrant must be specified in a greater level of detail than the simplified purposes of national security, prevention and detection of crime, and economic well-being.[21]

If a bulk interception warrant is likely to require the provision of assistance by a telecommunications operator outside the United Kingdom, the Secretary of State must consult the operator before issuing the warrant, and take into account the likely benefits of the warrant, the likely number of users to which the warrant relates, and the technical feasibility and likely cost of complying with the warrant.[22]

[13] Section 138(2)(b), Investigatory Powers Act 2016
[14] Section 138(3), Investigatory Powers Act 2016
[15] Section 138(4), Investigatory Powers Act 2016
[16] Section 138(1)(c), Investigatory Powers Act 2016
[17] Section 2(2)(a), Investigatory Powers Act 2016
[18] Section 142(4), Investigatory Powers Act 2016
[19] Section 138(1)(d), Investigatory Powers Act 2016
[20] Section 142(4), Investigatory Powers Act 2016
[21] Section 142(7), Investigatory Powers Act 2016
[22] Section 139, Investigatory Powers Act 2016

Subsequent to the Secretary of State issuing the warrant, a Judicial Commissioner ("JC") must approve the decision, reviewing the following matters:

- Whether the warrant is necessary;
- Whether the conduct that would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct;
- Whether each of the specified operational purposes is a legitimate purpose for which the examination of content or data is necessary.[23]

Although this process has been described as a "double lock", implying that there are two levels of authorisation inherent in each warrant approval, the JC's review is limited to the application of "judicial review principles", and compliance with general duties in relation to privacy specified in section 2 of the Act.[24] Whether the reference to "judicial review principles" is intended to imply a circumscription of the JC's role has been the subject of considerable debate and remains subject to interpretation. [25] During the legislative process then Home Secretary, now Prime Minister Theresa May, indicated the government's perspective that the JC should not be "retaking the decision. They are looking to see whether the original decision was flawed." However, amendments were later made suggesting that the "review will be an upper-end, stricter one… (of) close scrutiny."[26]

Bulk interception warrants cease to have effect after six months,[27] unless the warrant is renewed by the Secretary of State where they consider it necessary and proportionate to do so.[28] Warrants can be modified at any time to add, vary or remove any operational purpose for which content or data may be selected for examination.[29] Such a modification constitutes a "major modification", which must be approved by a Judicial Commissioner, applying the same standard as approval of warrants.[30] Major modifications can be approved by the Secretary of State only in

[23] Section 140(1), Investigatory Powers Act 2016
[24] Section 140(2)
[25] Byron Karemba, "The Investigatory Powers Bill: Introducing Judicial Authorisation of Surveillance Warrants in the United Kingdom – Putting the "Doubel-Lock" in Focus (Part I), *UK Constitutional Law Association Blog,* 22 March 2016, available at https://ukconstitutionallaw.org/2016/03/22/byron-karemba-the-investigatory-powers-bill-introducing-judicial-authorisation-of-surveillance-warrants-in-the-united-kingdom-putting-the-double-lock-in-focus-part-i/
[26] Column 885, Hansard 06 June 2016 Volume 611
[27] Section 143, Investigatory Powers Act 2016
[28] Section 144, Investigatory Powers Act 2016
[29] Section 145, Investigatory Powers Act 2016
[30] Section 146, Investigatory Powers Act 2016

cases of urgent need, provided that they are subsequently approved by a Judicial Commissioner within three days.[31]

Safeguards

The Secretary of State must ensure that there are arrangements in force for ensuring that

- The number of persons to whom material is disclosed, the extent to which material is disclosed or copied, and the number of copies that are made, is limited to the minimum necessary;[32]
- Every copy made of material is stored, for so long as it is retained, in a secure manner;[33] and
- Every copy made of material is destroyed as soon as there are no longer any relevant grounds for retaining it;[34] that is, that the retention is not necessary or likely to become necessary in the interests of national security or other grounds specified in the warrant.[35]

The selection of intercepted content or secondary data for examination can only be done for the operational purposes specified in the warrant,[36] and must be necessary and proportionate in all the circumstances.[37] Content (but not secondary data) cannot be selected for examination where the following two conditions exist:

- where any criteria used for the selection of content for examination are referable to an individual known to be in the British Islands at that time; and
- where the purpose of using those criteria is to identify the content of communications sent by, or intended for, that individual.[38]

There are two exceptions to this prohibition: where there is a change of circumstances during the selection for examination, for example where a person enters the British Islands during the

[31] Section 147(3), Investigatory Powers Act 2016
[32] Section 150(1)(a) and (2), Investigatory Powers Act 2016
[33] Section 150(4), Investigatory Powers Act 2016
[34] Section 150(5), Investigatory Powers Act 2016
[35] Section 150(6), Investigatory Powers Act 2016
[36] Section 152(2), Investigatory Powers Act 2016
[37] Section 152(1)(b), Investigatory Powers Act 2016
[38] Section 152(4), Investigatory Powers Act 2016

examination,[39] and where a targeted examination warrant is obtained under section 15(1)(b) of the Act. A targeted examination warrant authorises the selection of relevant content in breach of the British Islands prohibition.[40] Despite having the word "targeted" in its name, a targeted examination warrant may relate to a group of persons who share a common purpose, more than one person or organisation, or more than one set of premises.[41] Targeted examination warrants are subject to similar authorisation requirements and procedures as bulk interception warrants.[42]

There are limited additional safeguards for items subject to legal privilege and journalistic confidentiality. A senior official acting on behalf of the Secretary of State must approve any criteria used for selection for examination likely to identify legally privileged items, or specifically targeting items subject to legal privilege.[43] Where a communication intercepted in accordance with a bulk interception warrant is retained, following its examination, and it contains confidential journalistic material, the agency in whose name the warrant is issued must inform the Investigatory Powers Commissioner as soon as is reasonably practicable.[44]

Bulk Equipment Interface

A supplementary mechanism for getting access to bulk communications content and data is through what the Investigatory Powers Act calls bulk "equipment interference", but which might otherwise be known as bulk "hacking", "intrusion" or "computer network exploitation." Under British law, intelligence agencies may obtain bulk equipment interference warrants in order to acquire the content of communications, as well as equipment data, which is comprised of systems data (data associated with the communications being acquired) and identifying data, data associated with a communication but which can be logically separated from it.[45] Identifying data might include, for example, the location of a meeting in a calendar appointment, or the time and date that a photograph was taken.[46]

[39] Section 152(5) and (6), Investigatory Powers Act 2016
[40] Section 15(3), Investigatory Powers Act 2016
[41] Section 17(2), Investigatory Powers Act 2016
[42] See section 19, Investigatory Powers Act 2016
[43] Section 153, Investigatory Powers Act 2016
[44] Section 154, Investigatory Powers Act 2016
[45] Section 177, Investigatory Powers Act 2016
[46] Equipment Interference Code of Practice, February 2017 Draft, para. 2.4.

Requirements for authorisation

The authorisation regime for bulk equipment interference ("bulk EI") is broadly similar to that applicable to bulk interception. Warrants can only be obtained by intelligence agencies when the main purpose is obtaining overseas-related communications, information, or equipment data.[47] Bulk EI warrants cover both the equipment interference and the selection for examination of any material obtained under the warrant.[48]

The Secretary of State may issue a warrant where the following conditions are met:

- The warrant is necessary either
  - in the interests of **national security**;[49]
  - for the purpose of **preventing and detecting serious crime**;[50]
  - in the interests of the **economic well-being of the United Kingdom** so far as those interests are relevant to the interest of national security[51] provided that the information which it is considered necessary to obtain is information relating to the acts or intentions of persons outside the British Islands;[52]
- The conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.[53]
- The warrant specifies the operational purposes for which any intercepted content or equipment data obtained under the warrant may be selected for examination,[54] and the Secretary of State is satisfied that each of the specified operational purposes is a purpose for which the examination may be necessary.[55] The operational purposes must be ones specified in a list maintained by the heads of the intelligence services as acceptable operational purposes,[56] and in the warrant must be specified in a greater level of detail

[47] Section 176, Investigatory Powers Act 2016
[48] Section 176(4)(b) Investigatory Powers Act 2016
[49] Section 178(1)(b)(i), Investigatory Powers Act 2016
[50] Section 178(2)(a), Investigatory Powers Act 2016
[51] Section 178(2)(b), Investigatory Powers Act 2016
[52] Section 178(3), Investigatory Powers Act 2016
[53] Section 178(1)(c), Investigatory Powers Act 2016
[54] Section 183(4), Investigatory Powers Act 2016
[55] Section 178(1)(d), Investigatory Powers Act 2016
[56] Section 183(5), Investigatory Powers Act 2016

than the simplified purposes of national security, prevention and detection of crime, and economic well-being.[57]

Bulk EI warrants are also subject to approval by a JC, who must apply judicial review principles[58] to the following matters:

- Whether the warrant is necessary;
- Whether the conduct that would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct;
- Whether each of the specified operational purposes is a legitimate purpose for which the examination of content or data is necessary.[59]

Warrants can be issued without the approval of a JC in urgent cases, in which case the JC must retroactively approve the warrant within three days.[60]

Bulk EI warrants have a duration of six months from when they were issued, except for urgent warrants which expire after five days.[61] The renewal and modification procedures are the same as those applicable to bulk interception.

Safeguards

As with bulk interception, the Secretary of State must ensure that in relation to every bulk EI warrant, there are arrangements in force for ensuring that

- The number of persons to whom material is disclosed, the extent to which material is disclosed or copied, and the number of copies that are made, is limited to the minimum necessary.[62] In this regard the bulk EI provisions are somewhat broader than those applicable to bulk interception: material may be disclosed and copied if it is necessary for purposes

[57] Section 183(8), Investigatory Powers Act 2016
[58] Section 179(2), Investigatory Powers Act 2016
[59] Section 179(1), Investigatory Powers Act 2016
[60] Section 180, Investigatory Powers Act 2016
[61] Section 184, Investigatory Powers Act 2016
[62] Section 191 (1) and (2), Investigatory Powers Act 2016

beyond the authorised purposes, such as for legal proceedings or for the performance of the functions of any person under any enactment.[63]

- Every copy made of material is stored, for so long as it is retained, in a secure manner;[64] and
- Every copy made of material is destroyed as soon as there are no longer any relevant grounds for retaining it;[65] that is, that the retention is not necessary or likely to become necessary in the interests of national security or other grounds specified in the warrant.[66]

The same requirements apply to bulk EI as apply to bulk interception when it comes to selection for examination: material can be accepted for examination without obtaining a further warrant where the criteria used for examination are not referable to an individual known to be in the British Islands at that time, and where the purpose of using those criteria is to identified communications sent by or intended for that individual.[67] Otherwise, a targeted examination warrant is required.[68]

As with bulk interception warrants, there are limited safeguards in place for items subject to legal privilege[69] and confidential journalistic material.[70] An additional protection is in place for members of parliament: if a targeted examination warrant is sought and it has, as its purpose, the selection for examination of material which consists of communications sent by, or intended for, a member of the legislature, or which consists of a member of parliament's private information, the Prime Minister must approve the warrant.[71] In terms of retention and destruction, the agency conducting bulk EI must specify the maximum retention periods for different categories of the data, which reflect its nature and intrusiveness. Those periods should normally be no longer than two years, and should be agreed with the Investigatory Powers Commissioner.[72]

[63] Section 191 (3), Investigatory Powers Act 2016
[64] Section 150(4), Investigatory Powers Act 2016
[65] Section 150(5), Investigatory Powers Act 2016
[66] Section 150(6), Investigatory Powers Act 2016
[67] Section 193, Investigatory Powers Act 2016
[68] Section 191 (1) and (2), Investigatory Powers Act 2016
[69] Section 194, Investigatory Powers Act 2016
[70] Section 195, Investigatory Powers Act 2016
[71] Section 111, Investigatory Powers Act 2016
[72] Equipment Interference Code of Practice, February 2017 Draft, para. 9.28.

4. Data Retention and Acquisition

Bulk retention of Communications Data

The law pertaining to the mandatory retention of communications data by telecommunications operators is currently on shaky ground in the United Kingdom.

Part 4 of the Investigatory Powers Act purports to empower the Secretary of State to require telecommunications operators to retain communications data in bulk for up to twelve months, replicating the existing legislative framework provided for by emergency legislation DRIPA, which sunsetted at the end of 2016. However, DRIPA was subject to a legal challenge by Members of Parliament David Davis and Tom Watson, who argued that the legal regime therein conflicted with European law, namely the decision of the Court of Justice of the European Union ("CJEU") in *Digital Rights Ireland*.[73]

The Watson and Davis challenge was subject to a reference to the CJEU, which handed down its judgement mere weeks after the IP Act was adopted by parliament. The CJEU's Grand Chamber considered that the retention of communications data sanctioned by DRIPA "exceeds the limit of what is strictly necessary and cannot be considered to be justified, within a democratic society."[74] In particular, the Court took issue with the blanket nature of the retention; the fact that the legislation did not require a nexus between the data to be retained and a threat to public security, or restrict retention in relation to a particular time period, geographical area, or group of persons likely to be involved in a crime made the legislation incompatible with Articles 7 (privacy) and 8 (protection of personal information) of the European Charter of Fundamental Rights.[75] Furthermore, the Court stipulated that access of competent national authorities to retained data should "be subject to a prior review carried out either by a court or by an independent administrative body",[76] and that the

[73] Joined Cases C-293/12 and C-594/12, Judgement of 8 April 2014, available at http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=lst&docid=150642&occ=first&dir=&cid=314051.
[74] Joined Cases C-203/15 and C-698/15, Judgement of 21 December 2016, para. 107
[75] Joined Cases C-203/15 and C-698/15, Judgement of 21 December 2016, para. 106.
[76] Joined Cases C-203/15 and C-698/15, Judgement of 21 December 2016, para. 120.

persons affected by access to retained data should be notified as soon as such notification is no longer liable to jeopardise the investigation.[77]

The Court referred the case back to the English Court of Appeal for a decision on the extent to which UK law is consistent with EU requirements. As the IP Act currently stands, the Court of Appeal will have no choice but to declare aspects of it as inconsistent with EU law. The government declined to issue a Draft Code of Practice for Retention alongside the other codes of practice it issued in February 2017, indicating that it will await the decision of the domestic courts on the implications of the *Watson* decision before taking further steps in this regard.

Requirements for authorisation

Assuming the provisions of the IP Act remain in force until that time, the Secretary of State can presently issue a retention notice to a telecommunications operator requiring the retention of "relevant communications data" for up to twelve months[78] if they consider it necessary and proportionate[79] for one of the following purposes:

- in the interests of national security;
- for the purpose of preventing or detecting crime or of preventing disorder;
- 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;
- in the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department,
- 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,
- to identify persons who have died or unable to identify themselves or their next of kin because

[77] Joined Cases C-203/15 and C-698/15, Judgement of 21 December 2016, para. 121.
[78] Section 87(3) Investigatory Powers Act 2016
[79] Section 87(1)(a) Investigatory Powers Act 2016

of a physical or mental condition;

- the regulation of financial services and markets; or
- financial stability.[80]

Importantly, the Act notes that the fact that retained data relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establishing that the retention is necessary within one of the abovelisted categories.[81]

An important extension of the power to require the retention of communications data introduced by the IP Act concerns the expansion of the definition of "relevant communications data" beyond traffic data to include data which may be used to identify, or assist in identifying, the telecommunication system to which a communication is transmitted.[82] The legislation explicitly states that, therefore, the definition of relevant communications data includes "internet connection records." In the explanatory notes to the Investigatory Powers Bill, the government explained that internet connection records are a record of the services that an individual a specific device has connected to, such as a website or an instant messaging application.

Judicial Commissioners must approve retention notices, reviewing the Secretary of State's conclusions regarding the necessity and proportionality of the notice.[83] JCs should apply judicial review principles and comply with the general duties in relation to privacy.[84] If the JC refuses to approve a decision, the Secretary of State can ask the Investigatory Powers Commissioner to approve the decision instead.[85]

Retention notices may relate to retention of all data or a description of data, and to a particular operator or a description of operators,[86] but must not require an operator who controls a telecommunication system to retain data which relates to the use of another telecommunication

[80] Section 61(7) Investigatory Powers Act 2016
[81] Section 87(10) Investigatory Powers Act 2016
[82] Section 87(11), Investigatory Powers Act 2016
[83] Section 89(1), Investigatory Powers Act 2016
[84] Section 89(2), Investigatory Powers Act 2016
[85] Section 89(4), Investigatory Powers Act 2016
[86] Section 87(2) Investigatory Powers Act 2016

operator in relation to that system.[87] Retention notices can include requirements to retain data in such a way that it can be transmitted efficiently and effectively in response to requests.[88]

Safeguards

Part 4 imposes obligations on telecommunications operators to secure the data, by appropriate technical and organisation measures, and make sure it can be accessed only by specially authorised persons. Telecommunications operators must also destroy the data after the retention of data ceases to be authorised.[89] They cannot disclose the existence or contents of the retention notice to any other person.[90]

Bulk Acquistion of Communications Data

Communications data retained by telecommunications operators can be accessed through one of two means: either through a targeted authorisation for obtaining communications data, issued under Part 3 of the Act, or a bulk acquisition warrant, for which intelligence agencies can apply under Part 6, Chapter 2 of the Act. In this section we analyse the bulk acquisition warrant procedure; however, it is worthwhile noting that Part 3 envisages that the Secretary of State may establish, maintain and operate "filtering arrangements" to enable police officers to submit and obtain communication data in response to targeted communication data requests. Although no further information has been published to date about how exactly such filtering arrangements would work, it is understood that they will encapsulate a technical system that enables police to interface with retained communications data directly, suggesting that it may entail the creating of a federated database of retained telecommunications data permitting a single search to query information retained by a number of different service providers. According to the government's explanatory notes on the Investigatory Powers Bill,

> "The filtering arrangements will minimise the interference with the right to privacy, in particular respect for personal correspondence, to which requests for internet based communications data

[87] Section 87(4) Investigatory Powers Act 2016
[88] Section 87(9), Investigatory Powers Act 2016
[89] Section 92, Investigatory Powers Act 2016
[90] Section 95(3), Investigatory Powers Act 2016

will give rise thereby ensuring that privacy is properly protected. In practice, filtering arrangements would be implemented by the Secretary of State in a Request Filter system which would be used by public authorities granting authorisations for the targeted acquisition of communications data."

Although targeted requests for data through the filter are outside the scope of this study, it will be important to monitor the implementation of the filtering arrangements, given the potential for the use of technical data retrieval system to transform, over time, into another form of untargeted or passive surveillance.

Requirements for authorisation

The Secretary of State may issue a warrant for bulk acquisition of communications data where the following conditions are met:

- The warrant contains a provision stating that it is a bulk acquisition warrant,[91] and is addressed to the head of the intelligence service by whom, or on whose behalf, the application is made;[92]
- The warrant is necessary either
  - in the interests of **national security**,[93]
  - for the purpose of **preventing and detecting serious crime**,[94]
  - in the interests of the **economic well-being of the United Kingdom** so far as those interests are relevant to the interest of national security[95] provided that the information which it is considered necessary to obtain is information relating to the acts or intentions of persons outside the British Islands,[96]
- The conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.[97] In considering whether a bulk acquisition warrant is necessary and proportionate, the

[91] Section 161(1), Investigatory Powers Act 2016
[92] Section 161(2), Investigatory Powers Act 2016
[93] Section 158 (1)(a)(i), Investigatory Powers Act 2016
[94] Section 158(2)(a), Investigatory Powers Act 2016
[95] Section 158(2)(b), Investigatory Powers Act 2016
[96] Section 158(3), Investigatory Powers Act 2016
[97] Section 158(1)(c), Investigatory Powers Act 2016

Secretary of State must take into account whether what is sought to be achieved by the warrant could reasonably be achieved by other less intrusive means;[98] and

- The warrant specifies the operational purposes for which any communications data obtained under the warrant may be selected for examination,[99] and the Secretary of State is satisfied that each of the specified operational purposes is a purpose for which the examination may be necessary.[100] The operational purposes must be ones specified in a list maintained by the heads of the intelligence services as acceptable operational purposes,[101] and in the warrant must be specified in a greater level of detail than the simplified purposes of national security, prevention and detection of crime, and economic well-being.[102]

That the retained data relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establishing that the retention is necessary within one of the abovelisted categories.[103] A bulk acquisition warrant may relate to data that is not in existence at the time of issuing the warrant.[104]

Bulk acquisition warrants are also subject to approval by a JC, who must apply judicial review principles[105] to the following matters:

- Whether the warrant is necessary;
- Whether the conduct that would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct;
- Whether each of the specified operational purposes is a legitimate purpose for which the examination of content or data is necessary.[106]

If the JC refuses to approve a decision, the Secretary of State can ask the Investigatory Powers Commissioner to approve the decision instead.[107]

[98] Section 2(2)(a), Investigatory Powers Act 2016
[99] Section 161(4), Investigatory Powers Act 2016
[100] Section 158(1)(d), Investigatory Powers Act 2016
[101] Section 161(4), Investigatory Powers Act 2016
[102] Section 161(7), Investigatory Powers Act 2016
[103] Section 87(10) Investigatory Powers Act 2016
[104] Section 158(9), Investigatory Powers Act 2016
[105] Section 159(2), Investigatory Powers Act 2016
[106] Section 159(1), Investigatory Powers Act 2016

Provisions regarding the duration,[108] renewal,[109] modification,[110] implementation,[111] and service of warrants[112] are the same as applies to the other bulk powers detailed above.

Safeguards

However, the examination regime applicable to bulk acquisition warrants differs from that applicable to bulk interception and bulk EI. There is no probation on searching the acquired communications data using criteria referable to a person known to be in the British Islands, and a targeted examination warrant is not required in any circumstances.[113] Rather, data can be examined if it is necessary for the operational purposes outlined in the warrant, and if it is necessary and proportionate in all the circumstances.[114]

The safeguards applicable to retention and disclosure of data are broadly the same as other bulk provisions.[115]

Bulk Acquisition and Retention of Personal Datasets

Under the Intelligence Services Act 1994, intelligence agencies may acquire and retain "bulk personal datasets", sets of personal information about a large number of individuals who are not and are unlikely to become of interest to the intelligence agencies. Such datasets may be acquired overtly or covertly, from public sector bodies or commercially from the private sector.

Prior to the introduction of the Investigatory Powers Act, the agencies were acquiring such datasets on the basis of authorities which, on their face, did not suggest such a practice was underway. The

[107] Section 159(4), Investigatory Powers Act 2016
[108] Section162, Investigatory Powers Act 2016
[109] Section163, Investigatory Powers Act 2016
[110] Section164, Investigatory Powers Act 2016
[111] Section168, Investigatory Powers Act 2016
[112] Section169, Investigatory Powers Act 2016
[113] Section172, Investigatory Powers Act 2016
[114] Section172(1), Investigatory Powers Act 2016
[115] Section171, Investigatory Powers Act 2016

IP Act introduces new safeguards regulating to use of bulk personal datasets into statute for the first time.

Requirements for Authorisation

The authorisation provisions pertaining to bulk personal datasets ("BPDs") specify that bulk personal dataset warrants only apply where intelligence agencies seek to retain or examine a bulk personal dataset that hasn't been acquired under other provisions in the IP Act.[116] Where intelligence agencies do obtain bulk personal datasets under a warrant issued under the Act, other than a bulk acquisition warrant, they may apply for a direction of the Secretary of State authorising the retention or examination of the bulk personal dataset.[117]

With respect to all other datasets that come into the agencies' possession, there are provisions in the Act which permit an initial examination of a dataset which an intelligence service believes may include personal data on a number of individuals who are not, and are unlikely to become, of interest to the intelligence service.[118] The intelligence service has three months from when they begin examining the dataset (if the dataset was created in the United Kingdom; six months if it was created outside the United Kingdom) to decide whether to retain the set, and apply for a BPD warrant.[119]

A warrant is required to retain or examine a bulk personal dataset.[120] There are two classes of warrants: a class BPD warrant, which authorises an intelligence agency to retain, or retain and examine, any BPD of a class described in the warrant, and a specific BPD warrant, which pertains only to a BPD described in the warrant.

Class warrants

BPDs cannot be retained and examined in reliance on a class BPD warrant if the head of the intelligence agency considers that:

[116] Section 201(1), Investigatory Powers Act 2016
[117] Section 225, Investigatory Powers Act 2016
[118] Section 220, Investigatory Powers Act 2016
[119] Section 220, Investigatory Powers Act 2016
[120] Section 200(1) and (2), Investigatory Powers Act 2016

- the BPD consists of, or includes, protected data.[121] Protected data means, essentially, private information, and excludes systems data, metadata and other separable data;[122]
- the BPD consists of, or includes, health records;[123]
- a substantial proportion of the bulk personal dataset consists of sensitive personal data;[124] or
- the nature of the BPD, or the circumstances in which it was created, are such that it raises novel or contentious issues which ought to be considered by the Secretary of State and a Judicial Commissioner under a specific BPD warrant.[125]

The Secretary of State may issue a class BPD warrant where

- the warrant is necessary either
  - in the interests of **national security**,[126]
  - for the purpose of **preventing and detecting serious crime**,[127]
  - in the interests of the **economic well-being of the United Kingdom** so far as those interests are relevant to the interest of national security[128]
- The conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct;[129] and
- Where the warrant authorises examination of BPDs in a particular class, it specifies the operational purposes for which data contained in BPDs under the warrant may be selected for examination.[130] The operational purposes must be ones specified in a list maintained by the heads of the intelligence services as acceptable operational purposes,[131] and in the warrant must be specified in a greater level of detail than the simplified purposes of national security, prevention and detection of crime, and economic well-being.[132]

[121] Section 202(1), Investigatory Powers Act 2016
[122] Section 203, Investigatory Powers Act 2016
[123] Section 202(2)(a), Investigatory Powers Act 2016
[124] Section 202(2)(b), Investigatory Powers Act 2016
[125] Section 202(3), Investigatory Powers Act 2016
[126] Section 203(3)(a)(i), Investigatory Powers Act 2016
[127] Section 204(3)(a)(ii), Investigatory Powers Act 2016
[128] Section 204(3)(a)(iii)), Investigatory Powers Act 2016
[129] Section 204(b), Investigatory Powers Act 2016
[130] Section 212(3), Investigatory Powers Act 2016
[131] Section 212 (5), Investigatory Powers Act 2016
[132] Section 212(8), Investigatory Powers Act 2016

A Judicial Commissioner must review the Secretary of State's conclusions regarding necessity and proportionality, including whether examination is necessary to meet the operational purposes described in the warrant.[133] In doing so, the JC must apply judicial review principles, and comply with general duties in relation to privacy.[134] If the JC refuses to approve a decision, they must provide written reasons, and the Secretary of State may ask the Investigatory Powers Commissioner to approve the decision instead.[135]

Specific warrants

Specific BPD warrants will be issued in two cases:

- Where the intelligence service is seeking authorisation to retain and examine a BPD which does not fall within a class described in a class warrant; or
- Where the intelligence service is seeking authorisation to retain and examine a BPD which falls within a class described but either
  - The intelligence service is prevented from retaining and examining the BPD (under the conditions enumerated above) or
  - The intelligence service considers it appropriate to seek a specific BPD warrant.[136]

The Secretary of State may issue a specific BPD warrant where

- the warrant is necessary either
  - in the interests of **national security**,[137]
  - for the purpose of **preventing and detecting serious crime**,[138]
  - in the interests of the **economic well-being of the United Kingdom** so far as those interests are relevant to the interest of national security[139]
- The conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct;[140]

[133] Section 208 (1), Investigatory Powers Act 2016
[134] Section 208(2), Investigatory Powers Act 2016
[135] Section 208 (3) and (4), Investigatory Powers Act 2016
[136] Section 205, Investigatory Powers Act 2016
[137] Section 205(6)(a)(i), Investigatory Powers Act 2016
[138] Section 205(6)(a)(ii), Investigatory Powers Act 2016
[139] Section 205(6)(a)(iii), Investigatory Powers Act 2016
[140] Section 205(b), Investigatory Powers Act 2016

- Where the warrant authorises the retention or examination of other BPDs that do not exist at the time of the issue of the warrant but which may be regarded as replacements for the dataset requested ("replacement datasets")[141], it includes a description that will enable those datasets to be identified;[142] and
- Where the warrant authorises examination of a BPD or a replacement dataset, it specifies the operational purposes for which data contained in the BPD and any replacement dataset under the warrant may be selected for examination.[143] The operational purposes must be ones specified in a list maintained by the heads of the intelligence services as acceptable operational purposes,[144] and in the warrant must be specified in a greater level of detail than the simplified purposes of national security, prevention and detection of crime, and economic well-being;[145]

A Judicial Commissioner must review the Secretary of State's conclusions regarding necessity and proportionality, including whether examination is necessary to meet the operational purposes described in the warrant.[146] In doing so, the JC must apply judicial review principles, and comply with general duties in relation to privacy.[147] If the JC refuses to approve a decision, they must provide written reasons, and the Secretary of State may ask the Investigatory Powers Commissioner to approve the decision instead.[148]

There are particular provisions in place for the issuing of urgent specific BPD warrants in section 209 and 210 of the Act. Provisions regarding the duration,[149] renewal,[150] and modification[151] are the same as applies to the other bulk powers detailed above. There are also new provisions regarding

[141] Section 205(8), Investigatory Powers Act 2016
[142] Section 212(4), Investigatory Powers Act 2016
[143] Section 212(4), Investigatory Powers Act 2016
[144] Section 212 (5), Investigatory Powers Act 2016
[145] Section 212(8), Investigatory Powers Act 2016
[146] Section 208 (1), Investigatory Powers Act 2016
[147] Section 208(2), Investigatory Powers Act 2016
[148] Section 208 (3) and (4), Investigatory Powers Act 2016
[149] Section 213, Investigatory Powers Act 2016
[150] Section 214, Investigatory Powers Act 2016
[151] Section 215, Investigatory Powers Act 2016

the cancellation of warrants,[152] and the non-renewal of warrants within the time period, which permits the reauthorisation of the warrant within five days.[153]

Safeguards

The Secretary of State must ensure that there are arrangements in place to ensure that the selection of data in BPDs for examination is carried out only so far as is necessary for the operational purposes specified in the warrant,[154] and in any event that it is necessary and proportionate in all the circumstances.[155] Furthermore, when a specific BPD warrant is issued in relation to protected data – basically, personal information – the Secretary of State may impose conditions which must be satisfied before the protected data may be selected for examination on the basis of criteria which are referable to an individual known to be in the British Islands at the time of the selection.[156]

The IP Act also contains additional safeguards for health records in the context of BPDs. Where the purpose of a specific BPD is to authorise the retention and examination of health records, the Secretary of State must consider that there are exceptional and compelling circumstances that make it necessary to authorise the retention and examination.[157] Additional safeguards are also present where the purpose of selection for examination is to identify items subject to legal privilege, or the search criteria is likely to identify such items. If such searches pertain to individuals known to be in the British Islands, the search criteria must be approved by the Secretary of State, and approved by a Judicial Commissioner.[158]In all other cases, it must be approved by a senior official acting on behalf of the Secretary of State.[159] The process for approving such requests is outlined in section 222 and 223 of the Act.

[152] Section 218, Investigatory Powers Act 2016
[153] Section 219, Investigatory Powers Act 2016
[154] Section 221(1) and (2), Investigatory Powers Act 2016
[155] Section 221 (1), Investigatory Powers Act 2016
[156] Section 207, Investigatory Powers Act 2016
[157] Section 206(3), Investigatory Powers Act 2016
[158] Section 222(2) and (4), Investigatory Powers Act 2016
[159] Section 222(3) Investigatory Powers Act 2016

5. Open-source Intelligence

UK law enforcement and intelligence agencies use both open source intelligence ("OSINT") and social media intelligence ("SOCMINT"). OSINT refers to the acquisition and analysis of all information that is in the public domain, such as websites, blogs and many specific open source data and service providers. SOCMINT refers to the acquisition and analysis of information from social media platforms. The two terms are used interchangeably, given that in many cases social media information is also in the public domain. However, actors such as NGO Privacy International have argued that whereas OSINT relates to content that is more clearly intended and available for everyone to read and watch, social media users generate and upload data within a range of different contexts, from person-to-person, person-to-group, group-to-group, all of which can be private or public interactions.

In his landmark report on UK surveillance law, *A Question of Trust*, Independent Reviewer of Terrorism Legislation David Anderson UK observed that
"UK law enforcement and security and intelligence agencies of course use OSINT, though the extent of that use is not publicly known. By way of example, following a review by the Her Majesty's Inspectorate of Constabulary of the August 2011 disorders in English cities, an "*all-sources hub*" was created to help police to tackle disorder, which includes social media monitoring."[160]

Guidance produced by the Association of Chief Police Officers of England, Wales, and Northern Ireland on the policing of anti-fracking protest in 2011 suggests that, "Social media is a vital part of any ... intelligence picture."[161] A 2013 report suggested that a staff of 17 officers in the National Domestic Extremism Unit was conducting SOCMINT on tweets, YouTube videos, and Facebook profiles.[162]

It is not clear what legal authorities British law enforcement and intelligence agencies are using to

[160] David Anderson, *A Question of Trust: Report of the Investigatory Powers Review*, June 2015, para. 4.30
[161] Association of Chief Police Officers, "*Policing Linked to Onshore Oil and Gas Operations"*, at §4.7.3; available at: https://netpol.org/wp-content/uploads/2015/08/Onshore-Oil-and-Gas-Operations-2015.pdf
[162] Paul Wright, "Meet Prism's little brother: Socmint," *Wired,* 26 June 2013, available at http://www.wired.co.uk/article/socmint

authorise OSINT and SOCMINT activities. In his 2014-2015 Annual Report, the Chief Surveillance Commissioner simply repeated his view that "that just because this material is out in the open, does not render it fair game."[163] In his paper *#Intelligence*, former GCHQ Director Sir David Omand, along with co-authors Jamie Bartlett and Carl Miller, gave some insight into the potential conceptual approach to, and legislative basis for, SOCMINT:

"where social media activity is taking place in the digital 'public domain', accessing it is not in principle intrusive. Content that can be found by anyone who wishes to search for it, because it is freely and openly available (such as tweets) is, in an important sense, public. The ability to collect and analyse a named individual's tweets in this way is similar to 'directed surveillance' – carrying out surveillance on an individual in a public space. This is surveillance of a specific individual or individuals, and falls under the authorisation stipulations of RIPA 2000 part II to manage its potential harm, but is not technically intrusive and not comparable to interception as regulated under Part I. Under current guidelines, directed surveillance of people in a public space requires a relatively low level of authorisation and can be undertaken by a number of agencies. A similar approach might be taken for SOCMINT of this type."[164]

6. Oversight and Supervision

The IP Act creates a more cohesive oversight system than was previously in place, doing away with various non-parliamentary bodies – the Interception of Communications Commissioner, the Chief Surveillance Commissioner, and the Intelligence Services Commissioner – and creating a single Investigatory Powers Commissioner ("IPC"). The IPC, appointed by the Prime Minister on the joint recommendation of a number of high ranking judges, will be supported by Judicial Commissioners, who must be serving or former High Court judges, responsible for approving warrants and inspecting the use of powers under the Act.

In addition to the IPC, the parliamentary oversight mechanism, the Intelligence and Security Committee, will continue to exercise some oversight, namely the approval of the list of operational

[163] Office of Surveillance Commissioners Annual Report for 2014-15, at para. 5.72.
[164] David Omand, Jamie Barlett and Carl Miller, "#Intelligence", 2012, available at http://www.demos.co.uk/files/_Intelligence_-_web.pdf?1335197327

purposes every three months.[165] The Investigatory Powers Tribunal will continue to have jurisdiction over complaints arising under the Act.

The main functions of the Commissioners are elaborated at section 229 of the Act. An interesting new responsibility for the IPC is contained in section 231, namely the obligation to report errors. The Investigatory Powers Commissioner must inform a person of any relevant error relating to that person of which the Commissioner is aware if the Commissioner considers that:

- the error is a serious error, meaning that it has caused significant prejudice or harm to the person concerned,[166] and
- it is in the public interest for the person to be informed of the error.[167]

It is not sufficient that there has been a breach of a person's rights under the Human Rights Act 1998 to justify reporting an error.[168] In making the decision to report the error, the IPC must

- Consider the seriousness of the error and its effect on the person concerned;[169]
- Consider the extent to which disclosing the error would be contrary to the public interest or prejudicial to
    - national security;
    - the prevention or detection of crime;
    - the economic well-being of the Untied Kingdom; or
    - the continued discharge of the functions of any of the intelligence services.[170]
- Consult the public authority which made the error;[171] and
- If informing the person of the error, inform them of any rights to apply to the Investigatory Powers Tribunal, and provide such details as may be necessary to exercise those rights.[172]

[165] Provided for in multiple provisions under Part 6 – Bulk Warrants.
[166] Section 231 (2), Investigatory Powers Act 2016
[167] Section 231(1), Investigatory Powers Act 2016
[168] Section 231(3), Investigatory Powers Act 2016
[169] Section 231 (4)(a), Investigatory Powers Act 2016
[170] Section 231 (4)(b), Investigatory Powers Act 2016
[171] Section 231(5), Investigatory Powers Act 2016
[172] Section 231(6), Investigatory Powers Act 2016

A Judicial Commissioner must furnish the Investigatory Powers Tribunal with documents, information and other assistance as they may require in connection with the investigation of any matter by the Tribunal.[173]

[173] Section 232, Investigatory Powers Act 2016

7. Data Protection

Intelligence agencies

Section 28 of the Data Protection Act[174] permits the Secretary of State to certify the exemption of certain authorities from particular parts of the Act due to national security concerns. The Secretary of State has issued such certificates exempting GCHQ, MI6[175] and MI5[176] from the data protection principles, as well as provisions regarding subject access. More generally, the right of individuals to request access to data relating specifically to them, is subject to exemptions for the safeguarding of national security, which are applied on a case by case basis.

A 2014 memorandum of understanding on national security cases (Data Protection Act) between the Secretary of State for Justice (on behalf of Government Departments) and the Information Commissioner, who has oversight over the implementation of and compliance with the Data Protection Act, provides guidelines for cooperation between the Information Commissioner's Office and the security services. The MoU relates to the ICO's enforcement powers under sections 42 (Request for assessment) and 43 (Information notices) of the Act, with respect to instances in which the section 28 exemption for national security cases is relied upon in response to subject access requests. The MoU circumscribes the extent and scope of information required to be provided by the security services in response to requests for information from the ICO.

Law enforcement agencies

Personal data processed for the prevention or detection of crime are exempt from the first data protection principle, that is the requirement to process data fairly and lawfully. They are also exempt from subject access provisions in section 7 of the Data Protection Act, to the extent that that provision is likely to prejudice the prevention and detection of crime.[177]

[174] United Kingdom, HM Government (1998), *Data Protection Act 1998*, 16 July 1998, available at www.legislation.gov.uk/ukpga/1998/29.
[175] GCHQ and MI6 are dealt with jointly; certificate available at http://amberhawk.typepad.com/ files/blog-s.28-straw-certificate-gchq-sis-no.-2-2001.pdf.
[176] Certificate available at http://amberhawk.typepad.com/files/blog-s.28-blunkett-certificate-security-service-2001.pdf.
[177] Section 29, Data Protection Act 1998

Accordingly, data collected and retained by police is not subject to the requirement for fairness and lawfulness, but is still subject to the remaining data protection principles, such as those requiring use and purpose limitation, and technical and organizational security.

In May 2018, the new EU Directive on the processing of personal data by law enforcement will come into effect. The Directive appears to reinstate the requirement regarding fairness and lawfulness, as well as a number of new obligations regarding data processing in the law enforcement sphere. For example, the Directive requires Member States to ensure that police make a distinction between data collected regarding suspects, convicted criminals and victims (Article 6) and a distinction between personal data based on facts from personal data based on assessments (Article 7).

Importantly, the Directive will impact upon predictive policing and profiling activities undertaken by law enforcement agencies. Article 11 requires that decisions based solely on automated processing, including profiling, which produce an adverse legal effect concerning the data subject or significantly affects him or her must be prohibited unless authorised and accompanied by appropriate safeguards for the rights and freedoms of the data subject, including the right to obtain human intervention on the part of the controller (Article 11). The same article also prohibits profiling which results in discrimination.

The Human Rights, Big Data and Technology Project

Human Rights Centre,
University of Essex,
Colchester CO4 3SQ
+44 (0)1206 872877

@HRBDTNews
www.hrbdt.ac.uk