Interception of Communications in the UK Law: Developments and Relativity to the ECHR Jurisprudence

Dr. Sami Hamdan Al-Rawashdeh
Professor of Criminal Law, College of Law- Qatar University
samirawashdeh@qu.edu.qa
Dr. Yaser Yousef Khalaileh
Professor of Public International Law, College of Law- Qatar University
khalaileh@qu.edu.qa

Abstract

As the interception of private communications is now becoming one vital tool available for public surveillance authorities in combating criminal activities and the imposition of national security, the real exercise of this may, nevertheless, represent a serious threat to individual privacy. In the UK, the regulatory regime has witnessed a serious of modifications in a couple of decades. One might highlight the failure of the interception of communication regime under the Interception of Communications Act 1985 to reconcile competing demands of privacy and interests of security. Whether the 2000 Act and the updated framework under the 2016 Act addresses the question in a different fashion is also questionable. Hence, this paper is to determine whether these regimes have met the requirements of legality under the European system. Furthermore, it examines whether the requirements imposed by the European Convention on Human Rights requirements, namely the factors of 'necessity' and 'proportionality' are truly satisfied in the current UK legal system. Accordingly, it is argued that although the 2000 Act may represents a step towards the implementation of the principle of the legality and human rights legitimacy, it has, nonetheless, missed the opportunity to simplify the law, and was not clear in drawing the limit of the right of the state to intrude into the private life of citizens. In fact, this regime displays little respect for individual privacy. It is highly doubtful whether the introduced Act has gone through a process of human rights assessment and, therefore, the Act is likely to fall short of the requirements imposed by the European community. Indeed, the 2016 Act can be described as the biggest reform of the UK's surveillance regulation, yet, privacy experts have heavily criticized the measures it contains.

Keywords: Interception, Investigatory of Powers Act 2016, Privacy, European Convention.

1. Introduction

The interception of individuals' communications and the use of covert surveillance by public authorities constitute an important deterrent available to the police and security services in combating criminal activity and the protection of national security. However, they represent a serious threat to individual privacy. The technology of surveillance has increasingly become sophisticated, and the use by public agencies of methods of secret surveillance has raised many privacy issues.

In England, the incorporation of the European Convention of Human Rights into domestic law by the Human Rights Act 1998 imposes more demands on the State to respect private life as guaranteed by Article 8 of the European Convention. Furthermore, the "common law approach, that the police can do what they want as long it is not prohibited by law is no longer acceptable".[1] Hence, the need for a statutory framework intended to introduce regulation of the use of methods of secret surveillance has become a one pressing concern.

The first unsuccessful attempt to address the issue of balancing human rights and the State right in this respect took place in 1985 when the Interception of Communications Act 1985[2] was passed as result of the decision of the European Court of Human Rights in *Malone v United Kingdom*.[3] The Regulation of Investigatory Powers Act 2000[4] was one subsequent attempt to provide a comprehensive statutory framework for the legitimate interception of communications. This Act created, for the first time, a statutory framework to ensure that the law enforcement activities are properly regulated, externally supervised, and are compatible with the European Convention. The Act covered the interception of communications, the power to demand acquisition, disclosure of communications data, the use of covert surveillance and human intelligence sources, and the power to demand decryption of unintelligible materials. With the exception of part II, the Act applies to England, Wales, Northern Ireland and Scotland.

Thereafter, the Investigatory Powers Act 2016 was concluded to provide for an updated framework for the use of investigatory powers to obtain communications and communications data. These powers cover the interception of communications, the retention and acquisition of communications data, and equipment interference for obtaining communications and other data. As such, it is not lawful to exercise such powers other than as provided for by the Act. The Act also makes provision relating to the security and intelligence agencies' retention and examination of bulk personal datasets.

[1] Cape, E., 'Regulating Police Surveillance' (2000) 150 *New Law Journal* 452.
[2] Hereinafter the 1985 Act.
[3] (1985) 7 EHRR 14.
[4] Hereinafter the 2000 Act.

This Act governs the powers available to the state to obtain communications and communications data. It provides consistent statutory safeguards and clarifies which powers different public authorities can use and for what purposes. It sets out the statutory tests that must be met before a power may be used and the authorization regime for each investigative tool, including a new requirement for Judicial Commissioners to approve the issuing of warrants for the most sensitive and intrusive powers. The Act also creates a new IPC to oversee the use of these powers. Finally, the Act provides a new power for the Secretary of State to require, by notice, communications services providers to retain internet connection records. The main aim of this Act is to ensure that the exercise of the powers of interception and surveillance is compatible with the European Convention and Human Rights Act 1998.

The purpose of this research is to highlight the failure of the interception of communication regime under the Interception of Communications Act 1985 to reconcile competing demands of privacy and interests of security. The research address whether the old regime under the 2000 Act and updated framework under the 2016 Act have met the requirements of legality under the European Convention. Furthermore, it examines whether the European Convention's requirements of necessity and proportionality have been satisfied, and the extent to which remedial regime has succeeded in meeting the demands of Article 13 of the European Convention.

This research argues that although the 2000 Act "represents a step towards full implementation of the principle of the legality"[5] and "marks an important recognition, by Parliament and the government, of the legitimacy of claims under the Human Rights Act",[6] the old regime has missed the opportunity to simplify the law and to clarify the limits of the right of the state to intrude into the private life of citizens.[7] This regime displays little respect for individual privacy. It is highly doubtful that the Act has gone through a process of human rights assessment and, therefore, the Act is likely to fall short of the requirements imposed by Article 8.[8] The 2016 Act can be described as the biggest reform of the UK's surveillance regulation, yet, privacy experts have heavily criticized the measures it contains. Civil rights groups and those in opposition to the authorities overriding powers power say that the 2016 Act is intrusive and draconian.

[5] Feldman, D., *Civil Liberties and Human Rights in England and Wales* (Oxford: Oxford University Press, 2002) at 682.
[6] Ibid.
[7] Cape, E., 'Regulating Police Surveillance' (2000) 150 *New Law Journal* 452.
[8] Fenwick, H., 'Covert Surveillance under the Regulation Investigatory Powers Act 2000, Part II' (2001) 65 *Journal of Criminal Law* 521.

2. The Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 received Royal Assent on 28 July 2000 and came into force on 2 October 2000.[9] It replaces the Interception of Communications Act 1985, and established a new legal framework to govern the interception of communications via public postal systems, public telecommunications systems and private telecommunications systems in the United Kingdom. It provides for a statutory framework which regulates the use of covert surveillance and other investigative techniques. It also implements Article 5 of the EU Directive 97/66/EC concerning the processing of personal data and protection of privacy in the telecommunications sector.

2.1. Interception of Communications

The 2000 Act covers the public postal and public telecommunications networks as well as private telecommunications networks that includes, emails and internal computer networks connected to the Internet if these systems are connected to the public telecommunications network. The aim of this provision is to ensure that the Act meets the demands of the European Court ruling in *Halford* v UK, where the European Court held that that there had been a breach of both Art.8 and Art.13.[10]

An extensive body of case law on Art. 8 ECHR has been developed by the European Court of Human Rights. However, the Court has dealt specifically with the interception of internet communication In *Copland v United Kingdom* case[11]. The European Court of

[9] For discussion see Akdeniz, Y., "Regulation of Investigatory Powers Act 2000: part 1: Bigbrother.Gov.UK: State Surveillance in the Age of Information and Rights"[2001] *Criminal Law Review*: 73-90; Mirfield, P., "Regulation of Investigatory Powers Act 2000:Part2: Evidential Aspects" [2001] *Criminal Law Review*: 91-107.

[10] In this case, following a refusal to promote Ms. Halford at Merseyside Police, she commenced proceedings in the Industrial Tribunal claiming that she had been discriminated against on grounds of sex. Ms. Halford alleges that certain members of the Merseyside Police Authority launched a 'campaign' against her in response to her complaint to the Industrial Tribunal. This took the form of leaks to the press and interception of her telephone calls. She alleged that calls made from her home and her office telephones were intercepted for the purposes of obtaining information to be used against her in the discrimination proceedings. She claimed a breach of Article 8 of the ECHR. The European Court held that that there had been a breach of both Art.8 and Art.13. Article 8 could apply to telephone calls made from business premises as well as from home, and that Halford would have a reasonable expectation of privacy in relation to such calls since she ws not warned that they might be intercepted. There was a reasonable likelihood that calls made by Halford from her office had been intercepted and this amounted to an interference by a public authority within the meaning of Art.8(2). This interference could not be said to be in accordance with the law under Art.8 as the 1985 Act did not apply to such calls and there was no other provision to regulate their interception. However, Halford had not established a reasonable likelihood that calls from her home had been intercepted. Article 13 had been violated in that the 1985 Act did not apply to calls made through Merseyside Police's internal telephone system and had no other means of redress under UK law. (1997) 24 E.H.R.R. 523.

[11] Ms. Copland was employed by Carmarthenshire College from 1991 to 1999. The College was administered by the UK Government and was therefore a public body for which the Government was responsible under the European Convention on Human Rights. During her employment, Ms Copland's telephone, e-mail and Internet usage were monitored by the college to determine whether she was making excessive personal use of its resources. Ms. Copland alleged that the college's monitoring amounted to an interference with her right to respect for "private life" and "correspondence" under Article 8(1) of the

Human Rights (ECHR) considered whether Ms. Copland's right to respect for her private life and correspondence had been breached under Article 8(1) of the European Convention on Human Rights. In concluding its decision, the Court found that telephone calls from business premises were covered by the terms "private life" and "correspondence" and that e-mails sent from work, and information derived from the monitoring of personal Internet usage, should be protected under Article 8(1). As the applicant had been given no warning that her calls, e-mails or Internet usage would be monitored, the ECHR stated that it was reasonable for the applicant to expect that her privacy would be respected.[12] The ECHR also held that the collection and storage of personal information relating to her telephone calls, as well as her e-mail and Internet usage, without her knowledge, amounted to an interference with the applicant's right to respect for her private life and correspondence. The Court rejected the Government's submission that the College was authorized under its statutory powers to "do anything necessary or expedient" for the purpose of providing higher and further education. It noted that there were no provisions in existence at the time that governed or regulated the circumstances in which employers could monitor the use of telephone, e-mail and Internet by employees. As there was no domestic law regulating monitoring at this time, the interference in this case was not "in accordance with the law", as is required by Article 8(2).

Section 2 (2) of RIPA defines interception as follows: "a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he—

(a) so modifies or interferes with the system, or its operation,

(b) so monitors transmissions made by means of the system, or

(c) so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system, as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication".

In *R v E* case[13], the police, who were pursuing an investigation into suspected drug dealing, obtained permission under the Police Act 1977 and the Regulation of Investigatory Powers Act 2000 (RIPA) to place a covert listening device in the appellant's car. The device recorded words spoken by the appellant to other people in the car, words spoken by those

---

Convention. The Carmarthenshire College admitted that telephone calls were monitored by analyzing telephone bills and that Internet usage was monitored by analyzing websites visited and dates, times and duration of visits. At that time, the College had no policy regarding workplace monitoring. The ECHR held that there had been a violation of Ms. Copland's rights under Article 8(1) and awarded her 3000 Euro for non-pecuniary damage and 6000 Euro for costs and expenses. [2007] E.H.C.R. 253.

[12] See Vincents Okechukwu Benjamin, "Interception of internet communications and the right to privacy: an evaluation of some provisions of the Regulation of Investigatory Act against the jurisprudence of the European Court of Human Rights" (2007) European Human Rights Law Review 637-648.

[13] [2004] EWCA Crim 1243; [2004] 1 W.L.R. 3279; [2004] 4 WLUK 427 (CA (Crim Div)).

people to him and words spoken by the appellant when in the car and using a mobile telephone, although it did not record what was said by the person on the other end of the telephone. The appellant was charged with offences of conspiracy to supply controlled drugs. At a preparatory hearing, held pursuant to s.29 of the Criminal Procedure and Investigations Act 1996 , the judge ruled that evidence of the recordings made by the covert device was admissible but under s.35 of the1996 Act he granted the appellant leave to appeal that ruling. On the appeal it was submitted on behalf of the appellant that what had occurred amounted to "interception" of the telephone calls, which were either interceptions authorized by the Secretary of State under s.5 of RIPA , or, if not, they constituted an offence of unlawful interception and, either way, all the evidence of the product of the listening device was therefore inadmissible as a consequence of s.17 of RIPA . Alternatively, if there was an unlawful interception, the evidence ought to be excluded under s.78 of the Police and Criminal Evidence Act 1984 . In addition, it was submitted that RIPA was enacted in part to achieve compliance with European Directive 97/66/EC which called for protection against listening, storage and surveillance of communications as well as against tapping and the need to comply with the directive required a fresh approach the authorities. Reliance was also placed on the wording of the Codes of Practice issued under the 1997 Act and RIPA.

The Court of Appeal dismissed the appeal and held that the natural meaning of the expression "interception" denoted some interference or abstraction of the signal, whether it was passing along wires or by wireless telegraphy, during the process of transmission. The recording of a person's voice did not become an interception simply because what he said went not only into the recorder, but, by a separate process, was transmitted by a telecommunications system, which as defined by s.2(1) was any system that existed for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electromagnetic energy. What was recorded in this case was what happened independently of the operation of the telecommunications system; they were not recordings made in the course of transmission. The directive expressly permitted and Article 8 indirectly required measures judged necessary in member states for the enforcement of the criminal law and for the confidentiality of communications. They did not require that the protection afforded by member states by way of regulation of the confidentiality of communications should extend to a prohibition upon the giving in evidence, at a trial for a criminal offence, of the kind of material in question here, where it had been lawfully obtained in accordance with authority properly given. Accordingly, the directive and Article 8 were complied with by RIPA and neither required the altered construction of the expression "interception" contended for. The Codes of Practice issued under the 1997 Act and RIPA went further than the law as enacted required and could not prevail against the clear meaning of the statute.

It has been argued that the subtlety of this interpretation raises questions of legal certainty. The "court did not grapple with the problems this presented for its interpretation of what

amounted to an interception. Indeed, in rejecting the appellant's submission, the court conceded that although what was happening was independent of the operation of the telecommunications system, "the recordings were made, questions of milliseconds apart, at the same time as the accused's words were being transmitted'. This was consistent with the decision of the House of Lords in *R* v *Effick*.[14] Consideration of this approach demonstrates that the difference between when a communication is intercepted during the course of its transmission may depend on nothing more than how the recording is made; if recorded simultaneously (without the sound waves being converted and capable of being interpreted by the brain as words) an interception takes place. If there is a millisecond's delay and the conversion takes place, there is no interception. This distinction, whilst clearly sustainable, significantly undermines the value of the privacy interest at stake, as the law is presently drafted".[15]

Section 1(1) of the Act makes it an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communications in the course of its transmission. It is also an offence to intercept communications on a private telecommunications system.[16] The interception of communications offence is subject to two limitations. First, the interception has lawful authority if it is authorised by or under section 3, 4 or 5 or where it is exercised, in relation to any stored communication, for the purpose of obtaining information or of taking possession of any document or other property.[17] This case covers circumstances where, for example, a person has been arrested in possession of a pager, and the police have reason to believe that the messages sent previously to that pager may be of assistance in the case.[18] Secondly, interception of communication in the course of its transmission by means of a private telecommunication system is excluded from criminal liability if it is permitted by a person with a right to control the operation or the use of the system; or he has the express or implied consent of such a person to make the interception.[19] Examples of this type of activity are an individual using a second handset in a house to monitor a telephone call, and a large company in the financial sector routinely recording calls from the public in order to retain a record of transactions.[20]

The Act authorises certain kinds of interception without an interception warrant under section 3 in the following circumstances. First, where all parties to a communication have

[14] [1995] 1 AC 309.
[15] Simon McKay, "Regulation of Investigatory Act 2000, Part I: meaning of "interception" 2005, 69(2) Journal of Criminal Law 106-109 at 107-108.
[16] Section 1(2) of the Regulation of Investigatory Powers Act 2000.
[17] Section 1(5) of the Act.
[18] Explanatory Notes of the 2000 Act, para 24.
[19] Section 1(6) of the Act.
[20] Explanatory Notes of the 2000 Act, para 25.

consented to the interception.[21] Secondly, where the communication is one sent by, or intended for, a person who has consented to the interception and the surveillance by means of that interception has been authorised under Part II.[22] This situation might arise where a kidnapper is telephoning relatives of a hostage, and the police wish to record the call in order to identify or trace the kidnapper. The operation will be authorised as surveillance, rather than by means of an interception warrant.[23] The first two exceptions "removes a danger under the previous legislation that a person's right to privacy might be abrogated, without his knowledge and without his external control, by unilateral consent given by someone else".[24]

However, the Court of Appeal in *R v Hardy*,[25] held that the tape recordings of telephone conversations were not "interceptions" for the purpose of section 3 within the meaning of section 2(2) of the 2000 Act if the calls had been taped by one of parties to those calls and the recordings had not been made available to the third parties whilst being transmitted. It was the same as the secret recording by the officer of a conversation whilst meeting the suspect face to face. "Further restricting "interception" to cases where a third party is involved severely curtails the protection RIPA provides, and is difficult to reconcile with s.3. The fact that the recording is not made available instantaneously for a third party does not prevent it being an interception".[26]

Thirdly, conduct consisting in the interception of a communication is authorised if it is conduct by or on behalf of a person who provides a postal service or a telecommunications service for purposes connected with the provision or operation of that service or with the enforcement, in relation to that service, of any enactment relating to the use of postal services or telecommunications services.[27] This might occur, for example, where the postal provider needs to open a postal item to determine the address of the sender because the recipient's address is unknown.[28]

Fourthly, where the communication is intercepted in the course of its transmission by means of wireless telegraphy is authorised by the Secretary of State to intercept the telegraphy transmissions for the purpose connected with the issue of licences under the Wireless Telegraphy Act 1949, the prevention or detection of anything which constitutes

[21] Section 3(1) (a) and (b) of the Act.
[22] Section 3(2) (a) and (b) of the Act.
[23] Explanatory Notes of the 2000 Act, para 39.
[24] Feldman, D., *Civil Liberties and Human Rights in England and Wales* (Oxford: Oxford University Press, 2002) at 669.
[25] [2003] 1 Cr. App. R 30.
[26] Underhill, G., and Ormerod, D., 'Appeal, Abuse of Process, Evidence' [2003] *Criminal Law Review* 394 at 397.
[27] Section 3(3) (a) and (b) of the Act.
[28] Explanatory Note of the 2000 Act, para 40.

interference with wireless telegraphy, or the enforcement of any enactment contained in that Act or of any enactment not so contained that relates to such interference.[29]

Section 4 provides further various forms of lawful authority.[30] First, the interception takes place in the course of its transmission by means of a telecommunication system for the purpose of obtaining information about the communications of a person who, or who the interceptor has reasonable grounds for believing, is in a country or territory outside the United Kingdom, and the interception relates to the use of a telecommunications service provided to persons in that country or territory.[31] Secondly, the Secretary of State may by regulations authorise any such conduct described in the regulations as appears to him to constitute a legitimate practice reasonably required for the purpose of monitoring or keeping a record of communications for business purposes.[32]This has been implemented by the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Thirdly, the public authorities have the power to intercept the communications of prisoners and hospital premises.[33]

By virtue of section 5 of the Act the Secretary of State may issue a warrant authorising or requiring the person to whom it is addressed to secure the interception in the course of their transmission by means of a postal service or telecommunication system of the communications described in the warrant. The Secretary of State shall not issue an interception warrant unless he believes it is "proportionate" and "necessary" on one of the following grounds:[34] (a) in the interest of national security; (b) for the purpose of preventing or detecting serious crime; (c) for the purpose of safeguarding the economic well-being of the United Kingdom; (d) for the purpose, in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a warrant for the purpose of preventing or detecting serious crime, of giving effect to the provisions of any international mutual assistance agreement. The aim of this subsection is to allow the United Kingdom to comply with the Convention on Mutual Assistance in Criminal Matters between Member States of the European Union.[35]

Although section 5 recites the Convention language, it is clear that section 5 of the Act authorises a wide range of public authorities to intercept all kinds of communication of individuals on very wide grounds. Furthermore, there is no doubt that the exceptions to the warrant procedure under sections 3,4 and 5 are very broad, especially those under the

[29] Section 3(4), (5) of the Act.
[30] Section 4 of the Act.
[31] Section 4(1) of the Act.
[32] Section 4(2) of the Act.
[33] Section 4(4),(5) and (6) of the Act.
[34] Section 5(2) of the Act.
[35] Akdeniz, Y., Walker, C. and Taylor, N., 'Regulation of Investigatory Powers Act 2000' [2001] *Criminal Law Review* 76.

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. The Lawful Business Practice Regulations allow businesses to intercept without consent for purposes such as recording evidence of transactions, ensuring regulatory compliance, detecting crime or unauthorised use, and ensuring the operation of their telecommunication systems.

"The requirement of the "belief" of the Secretary of State as the condition precedent to the issuance of an interception warrant seems to be overly subjective".[36] The RIPA as it reads today does not have a requirement of the factual indication, which means that the officials applying for the warrant should at the very least establish a prima facie case for the necessity of the warrant. The subjective requirement of the "belief" of the Secretary of State seems also to amount to too wide a discretion and would run counter to the requirement under Art.8(2). Mere belief does not establish necessity. This is indeed a critical issue since the conditions that must be established before interception is authorized are one of the effective guarantees against arbitrary interference with the right to privacy.[37] "There is presently nothing in the Act that requires a narrow delimitation of the materials the interception of which is deemed necessary. The result is that a massively invasive interception could presently be carried out under the Act even where only a significantly less invasive interception is necessary. The realities of the days in which the Act was enacted may have made the present provisions acceptable but there has been progress in technology since then. Filters are now possible. Therefore the RIPA needs revision in this regard".[38]

According to section 11 of the Act, the Government can require the communication service providers to take all necessary procedures to assist in the interception process. Failure to comply with this duty is an offence.[39] Section 12 authorises the Secretary of State to impose obligations (backed by civil proceedings) on the public postal service and public telecommunication service providers for the purpose of providing technical assistance in relation to the interception process. Accordingly, the Act creates a negative image of telecommunication service providers especially Internet service providers as it makes them the "electronic narks of the state".[40]

---

[36] Vincents Okechukwu Benjamin, "Interception of internet communications and the right to privacy: an evaluation of some provisions of the Regulation of Investigatory Act against the jurisprudence of the European Court of Human Rights" (2007) European Human Rights Law Review 637-648 at 644.

[37] Vincents Okechukwu Benjamin, "Interception of internet communications and the right to privacy: an evaluation of some provisions of the Regulation of Investigatory Act against the jurisprudence of the European Court of Human Rights" (2007) European Human Rights Law Review 637-648 at 644.

[38] Vincents Okechukwu Benjamin, "Interception of internet communications and the right to privacy: an evaluation of some provisions of the Regulation of Investigatory Act against the jurisprudence of the European Court of Human Rights" (2007) European Human Rights Law Review 637 at 648.

[39] Section 11(7) of the Act.

[40] Akdeniz, Y., Walker, C. and Taylor, N., 'Regulation of Investigatory Powers Act 2000' [2001] *Criminal Law Review* 78.

A warrant shall not be considered necessary on the ground of safeguarding the economic well being of the United Kingdom unless the information which it is thought necessary to obtain is information relating to the acts or intentions of persons outside of the British Islands.[41] Although the interception warrant provisions under the new regime are similar to those in the Interception of Communications Act 1985, there are some significant changes. The interception warrant must name or describe either one person as the interception subject or a single set of premises.[42] Section 9 of the Act allows warrants to subsist for three months on the ground of preventing or detecting serious crime and for six months on the grounds of interest of national security or safeguarding the economic well-being of the United Kingdom. Derogation

The new regime does not address all form of interceptions of communications, especially those carried out by foreign agencies either within the United Kingdom or targeted at the United Kingdom.[43] The Act also fails to offer a statutory protection for privileged material and to lay down the special procedures to be followed if it is necessary to intercept material that falls into a particularly sensitive category.[44] Although section 15 provides safeguards and restrictions on use of intercepted material, it does not cover material obtained without warrant under sections 3 and 4. Moreover, the interception of communications process is not subject to judicial authorisation. In *Kopp v Switzerland*,[45] the European Court stated that it is astonishing that the task of interception of telephone calls is assigned to an official of the Post Office's legal department, who is a member of the executive, without supervision by an independent judge. [46]

The safeguards contained in the 2000 Act in relation to interception of communications have been circumvented in the light of the recent ruling in *R (NTL Group Ltd) v Ipswich Crown Court*.[47] In this case the Chief Constable of Suffolk applied for an order for the

[41] Section 5(5) of the Act.
[42] Section 8(1) of the Act.
[43] Akdeniz, Y., Walker, C. and Taylor, N., 'Regulation of Investigatory Powers Act 2000' [2001] *Criminal Law Review* 79.
[44] See Cm. 4368, 1999, Para. 7.16.
[45] (1999) 27 EHRR 91, para 46.
[46] The case of **Big brother Watch and others v UK, ([2018] 9 WLUK 157**) concerned complaints by journalists and rights organizations about three different surveillance regimes under the Regulation of Investigatory Powers Act 2000: (1) the bulk interception of communications; (2) intelligence sharing with foreign governments; and (3) the obtaining of communications data from communications service providers. The European Court of Human Rights held by a majority that the UK had breached the ECHR art.8 and art.10 by granting itself the right to intercept internet communications in bulk through the Regulation of Investigatory Powers Act 2000 s.8(4). Inadequate independent oversight of the selection and search processes, and the lack of safeguards meant that the UK could not rely on the derogation for measures which were "necessary in a democratic society".For discussion see Kirsty Hughes, "Mass surveillance and the European Court of Human Rights" (2018) 6 European Human Rights Law Review 589-599.
[47] [2003] Q.B. 131.

production of special procedure material in the form of email information from an email address over a specified period under section 9 and Schedule 1 of the Police and Criminal Evidence Act 1984. The claimant, a telecommunication company, were of the opinion that to comply with the request would involve them in committing an offence of unlawfully intercepting a communication in the course of its transmission contrary to section 1 of the 2000 Act. The court rejected NTL's argument and held that:

> [I]t is implicit in the terms of paragraph 11 of Schedule 1 to PACE that the body subject to an application under section 9 (here NTL) has the necessary power arising implicitly from the language of paragraph 11 of Schedule 1, read together with section 9, to take the action which they apparently have to take in order to conserve the communications by e-mail within the system until such time as the court decides whether or not to make an order. That being so, that implicit power provides the lawful authority for the purposes of section 1(5) of the 2000 Act and no offence will therefore be committed if NTL acts in accordance with paragraph 11 of Schedule 1 to PACE when served with an application under section 9. As already anticipated, no harm will be caused to any third party in consequence of this being done because, unless a judge is prepared to make the order and therefore remove the protection which would otherwise exist for third parties, the police have no right to be informed of the contents of the material retained by NTL. In addition, there is a further less significant protection for NTL in that the application itself can only be made to the judge with the approval of a senior police officer of superintendent level or above. The judge therefore came to the right conclusion in granting the application in this case and in refusing the cross-application of NTL. We would dismiss this application.[48]

2.2. Encryption

Encryption is "the use of some means to disguise or obscure the meaning of a message".[49] Computer technology has created the need for encryption to protect private communication and confidential information and to facilitate electronic e-commerce.[50] Part III of the Act deals with the power to require disclosure of any encrypted (protected) information. According to section 49(2) any person with the appropriate permission believes that a key to the protected information is in the possession of any person may, by notice to the person whom he believes to have possession of the key, impose a disclosure requirement in respect of the protected information. A disclosure requirement in respect of any protected information must be proportionate and necessary on the following grounds: (a) in the interests of national security; (b) for the purpose of preventing or detecting crime; or (c) in

[48] Ibid, paras. 24-25.

[49] Akdenize, A., 'Cryptography and Liberty: Can the Trusted Third Parties be Trusted? A Critique of the Recent UK Proposals' (1997) 2 *The Journal of Information, Law and Technology*, available at <http://elj.warwick.ac.uk/jilt/cryptog/97_2akdz>

[50] Akdenize, Y., 'Cryptography and Liberty: Can the Trusted Third Parties be Trusted? A Critique of the Recent UK Proposals' (1997) 2 *The Journal of Information, Law and Technology*, available at <http://elj.warwick.ac.uk/jilt/cryptog/97_2akdz>

the interests of the economic well-being of the United Kingdom.[51] The notice imposing a disclosure requirement in respect of any protected information must contain several elements.[52] Section 49 (8) prohibits making of any disclosure to any person other than the person giving the notice or such other person as may be specified in or otherwise identified by, or in accordance with, the provisions of the notice.

Section 49(9) states that a notice under this section shall not require the disclosure of any key which is intended to be used for the purpose only of generating electronic signatures. Although this subsection intends to protect the integrity of signature keys, it will very often fail to do so. "In many cryptographic products the same password (or key) is used for both signature and confidentiality purposes and this means that access to keys for protected information will also give access to signature keys".[53] This has been confirmed by paragraph 8.10 of the Draft Code of Practice which states that a key may be required to be disclosed under the terms of the 2000 Act where there are reasonable grounds to believe that key has been used for an electronic signature and, additionally, for confidentiality purposes.[54]

Hence this reduces trust and confidence in Internet security and undermines the development of e-commerce after enactment of the Electronic Communications Act 2000 that intends to facilitate such development.[55] The Justice and the Foundation for Information Policy Research[56]on the Draft of Electronic Communications Bill[57] concluded that there were serious concerns about the compliance of Part III of the Draft (Power to require the disclosure of keys to protected information) with requirements of Article 8 of the European Convention. Part III of the Electronic Communications Bills was subsequently withdrawn and reintroduced as Part III of the Regulation of Investigatory Powers Bill.

The effect of a section 49 notice imposing a disclosure requirement in respect of any protected information on a person who is in possession of both the protected information and the means of obtaining access to the information and of disclosing it in an intelligible form is that he is entitled to use any key in his possession to obtain access to the information or to put it into an intelligible form, and is required to make a disclosure of the information

[51] Section 49(3) of the Act.
[52] Section 49(4) of the Act.
[53] Cyber-Rights & Cyber-Liberties (UK), 'A Critique of Part III, Regulation of Investigatory Powers Bill' 11 July 2000, at < http://www.cyber-rights.org/reports/part-iii.htm>
[54] See the Draft Code of Practice on part III of the 2000 Act, Investigation of electronic data protected by encryption etc, 10 July 2000, at < http://www.homeoffice.gov.uk/oicd/ripbill.htm. >
[55] Gladman, R. B., Comments on Draft Home Office Code of Practice on Part III, 11 July 2000, at <htpp://www.cyber-rights.org/reports/p3copcom.pdf>.
[56] Available at http: www.fipr.org/ecomm99/ecommaud.html.
[57] Department of Trade and Industry, *Draft Electronic Communications Bill*, Cm. 4417 (London: DTI, 1999).

in an intelligible form.[58] According to section 50(2) a person subject to a requirement to make a disclosure of any information in an intelligible form must be taken to have complied with that requirement if he makes disclosure of any key to the protected information that is in his possession. Section 50(3) is very damaging since the trust and confidence in the use of public key cryptography for both confidentiality and signature purpose will be seriously undermined. It creates direct access to keys and hence to all the information that they are being used to protect.[59]

Section 51(4) of the Act specifies the situations in which direct access to a key can be required. A person must not give this direction unless he believes: (a) that there are special circumstances of the case which mean that the purposes for which it was believed necessary to impose the requirement in question would be defeated, in whole or in part, if the direction were not given; and (b) that the giving of the direction is proportionate to what is sought to be achieved by prohibiting any compliance with the requirement in question otherwise than by the disclosure of the key itself. Under Section 51(5) the matters to be taken into account in considering whether the requirement of subsection (4)(b) is satisfied in the case of any direction must include the extent and nature of any protected information and any adverse effect that the giving of the direction might have on a business carried on by the person on whom the disclosure requirement is imposed. This section does not offer effective restrictions on requirements for key disclosure because the scope of the phrase 'special circumstances' in section 51(4)(a) is not legally defined.[60] This might cause considerable doubt and concern about precise circumstances in which keys could be seized. Furthermore the breadth of the discretion conferred raises problems with regard to compliance with Article 8 of the Convention with respect for privacy and correspondence. Accordingly, all the procedures, standards and technical mechanisms required for the protection of seized keys must be set out in details in the Code of practice.[61]

Failure to comply with a section 49 notice is an offence under section 53. A person to whom a section 49 notice has been given is guilty of an offence if he knowingly fails, in accordance with the notice, to make the disclosure required by virtue of the giving of the notice. In proceedings against any person for an offence under this section, if it is shown that that person was in possession of a key to any protected information at any time before the time of the giving of the section 49 notice, that person shall be taken for the purposes of those proceedings to have continued to be in possession of that key at all subsequent

[58] Section 50(1) of the Act.
[59] Cyber-Rights & Cyber-Liberties (UK), 'A Critique of Part III, Regulation of Investigatory Powers Bill', at < http://www.cyber-rights.org/reports/part-iii.htm.
[60] Cyber-Rights & Cyber-Liberties (UK), "A Critique of Part III, Regulation of Investigatory Powers Bill" at, <http://www.cyber-rights.org/reports/part-iii.htm.
[61] Gladman, R. B., Comments on Draft Home Office Code of Practice on Part III, 11 July 2000, at <htpp://www.cyber-rights.org/reports/p3copcom.pdf>.

times, unless it is shown that the key was not in his possession after the giving of the notice and before the time by which he was required to disclose it.[62] It has been argued the presumption of continued ownership is incompatible with Article 6 of the European Convention and unfair since it places the burden of proof on the accused (not on the prosecution) to show that the key was not in his possession after the giving of the notice.[63] However, section 53(3) provides that a person shall be taken to have shown that he was not in possession of a key to protected information at a particular time if sufficient evidence of that fact is adduced to raise an issue with respect to it and the contrary is not proved beyond a reasonable doubt. Accordingly, the accused does not have to meet a very heavy responsive burden.[64]

Section 54 deals with the tipping-off offence. A person served with a section 49 notice, who becomes aware of it or of its contents, is required to keep secret the giving of the notice, its contents and the things done in pursuance of it. Under section 54(4) a person who makes a disclosure to any other person of anything that he is required by a section 49 notice to keep secret shall be guilty of an offence with a five year maximum penalty. Section 54(5) provides defences to the tipping-off offence if it is shown that: (a) the disclosure was effected entirely by the operation of software designed to indicate when a key to protected information has ceased to be secure; and (b) that person could not reasonably have been expected to take steps, after being given the notice or (as the case may be) becoming aware of it or of its contents, to prevent the disclosure. It has been argued that:[65]

> The tipping-off offence in respect of key seizure is effectively useless for its presumed purpose of preventing those whose keys are seized from tipping-off their colleagues about the Government interest. It has been accepted by the Government that a person whose keys are seized is free to issue a new key immediately although they cannot say that they have done this because of key seizure. But if, on all other occasions in which they issue a new key, they simply say 'here is my new key – my old key is now insecure but not as a result of key seizure', their criminal colleagues can immediately see that the absence of an explanation identifies a law enforcement interest.

Section 55(2) imposes duties on the investigative authorities to ensure that any key so disclosed is stored in a secure manner and that all records of a key so disclosed (if not destroyed earlier) are destroyed as soon as the key is no longer needed for the purpose of enabling protected information to be put into an intelligible form. It is worth mentioning

---

[62] Section 53(2) of the Act.
[63] Cyber-Rights & Cyber-Liberties (UK), 'A Critique of Part III, Regulation of Investigatory Powers Bill', at < http://www.cyber-rights.org/reports/part-iii.htm.
[64] Yaman Akdeniz, "Regulation of Investigatory Powers Act 2000' [2001] *Criminal Law Review* 82 at 88.
[65] See Cyber-Rights & Cyber-Liberties (UK), 'A Critique of Part III, Regulation of Investigatory Powers Bill', at < http://www.cyber-rights.org/reports/part-iii.htm.

that the requirements for the security of seized keys, which has been set out in section 55(2)(e) and (f), are very weak and not sufficient since the Act allows the person who seizes a key to provide only that protection he or she considers necessary. The majority of authorities have no experience with cryptography and they do not know what protection is needed.[66] It should also be noted that there are no criminal offences imposed on public authorities for the unauthorised revelation of keys.[67] The Draft Code of Practice on Part III of the Act fails also to provide confidence in the protection of seized keys since it does not provide any guidance of any kind on the design, development, implementation and operation of the procedures, standards and technical mechanisms needed to provide protection for keys.[68]

2.3. Scrutiny

The oversight and complaints mechanisms under the 1985 Act have been perpetuated. The system of scrutiny includes the Interception of Communications Commissioner who has a statutory responsibility to keep under review the exercise and performance of the powers and duties under Part I and Part III of the Act.[69] Section 59 of the Act extends the same system of scrutiny to the powers in section 5 to 7 of the Intelligence Services Act 1994. The jurisdiction of the Intelligence Services Commissioner does not cover Northern Ireland.[70] According to section 61 the Investigatory Powers Commissioner for Northern Ireland must keep under review the exercise and performance in Northern Ireland, by the persons on whom they are conferred or imposed, of any powers or duties under Part II of the Act. In England and Wales, the Chief Surveillance Commissioner must, in addition to his functions under the Police Act 1997, keep under review the exercise and performance of the powers and duties conferred or imposed under Part II, and the exercise and performance, by any person other than a judicial authority, of the powers and duties conferred or imposed, otherwise than with the permission of such an authority, by or under Part III.[71] The Prime Minister may, after consultation with the Chief Surveillance Commissioner, appoint as Assistant Surveillance Commissioners such number of persons as the Prime Minister considers necessary for the purpose of providing the Chief Surveillance Commissioner with assistance.[72] The role of the Commissioner is limited to

[66] Cyber-Rights & Cyber-Liberties (UK), 'A Critique of Part III, Regulation of Investigatory Powers Bill', at < http://www.cyber-rights.org/reports/part-iii.htm>

[67] Akdeniz, Y., Walker, C. and Taylor, N., 'Regulation of Investigatory Powers Act 2000' [2001] *Criminal Law Review* 89. See also the House of Commons Trade and Industry Committee, Fourteenth *Report on the Draft Electronic Communications Bill*, 1999-00 HC 862, (London: HMSO, 1999), para.34.

[68] See Paragraph 11.9 of the Draft of Code of Practice on Part III of the Act. See also An analysis of the Draft Code see Gladman, R. B., 'Comments on Draft Home Office Code of Practice on Part III', 11 July 2000, at < htpp://www.cyber-rights.org/reports/p3copcom.pdf>.

[69] Sections 57 and 58 of the Act.

[70] Section 59(2) of the Act.

[71] Section 62 of the Act.

[72] Section 63 of the Act.

retrospective review of the exercises of the 2000 Act.[73] The oversight process by the Commissioners has been criticised:

> Retrospective review is likely to be less rigorous than prior scrutiny and it may well be easier to satisfy the requirements of necessity and proportionality when armed with the incriminating results of the surveillance. This creates the risk that although the statutory authorisation regime may comply with Art.8, individual exercises of the investigatory powers could be unnecessary or disproportionate. A further concern is that not all authorisations are subject to scrutiny; only those selected at random by the Commissioner will be reviewed. Accordingly, a substantial number of authorisations may never be subject to any form of independent scrutiny…In addition to functional deficiencies, it is questionable whether the Commissioners have the time and resources necessary to provide effective oversight. Staffing shortages have been identified as major problems by both the Chief Surveillance and Interception Commissioners in their annual reports. Although the situation has improved as a result of staff increases, shortages are likely to reoccur with the substantial increase in duties that will occur when further Parts of RIPA enter into force.[74]

There is also an independent Tribunal established by section 65 of the Act to deal with complaints under section 7(1)(a) of the Human Rights Act 1998 (proceedings for actions incompatible with Convention rights), to consider and determine any complaints made to them, and to consider and determine any reference to them by any person that he has suffered detriment as a consequence of any prohibition or restriction under section 17 which prohibits disclosure of any of the contents of any intercepted materials or any communications data in *civil proceedings*. Thus, it is clear that there is no redress provided for detriment arising when evidence is excluded in *criminal proceedings* as a consequence of any prohibition or restriction by virtue of section 17. It also has the jurisdiction to hear and determine any other such proceedings as may be allocated to it in accordance with provision made by an order of the Secretary of State.

It has been argued that most of the criticisms that related to the oversight and complaints systems under the 1985 Act remain or have even been amplified. The basic limitations, which affect the Commissioner's role under the new regime, remain unchanged. The oversight process by the Commissioner under the 2000 Act is very "complex, with several different Commissioners covering activities which may in fact all be part of the same

[73] Intrusive surveillance which is subject to prior approval by a Surveillance Commissioner, except in urgency cases.
[74] Ferguson, G. and Wadham, J., 'Privacy and surveillance: A Review of the Regulation of the Investigatory Powers Act 2000' [2003] *European Human Rights Law Review* 101-108.

operation".[75] The Commissioner's annual report to Parliament does not provide a comprehensive scrutiny.[76]

Furthermore, the oversight mechanism by the Tribunal under the 2000 Act is limited. According to section 67(7) of the Act, the Tribunal has the power to award compensation and to make an order to quash or cancel any warrant or authorisation. It also has the jurisdiction to make an order requiring the destruction of any records of information which has been obtained in exercise of any power conferred by a warrant or authorisation. Thus, the Tribunal's power to award remedies is discretionary.[77] However, the Tribunal does not have the power to give reasons for its decisions[78]or to make a declaration of incompatibility. This decreases substantially the possibility of identifying the abuse or protecting the applicant's rights.[79] Another shortcoming is that the determinations, awards, orders and other decisions of the Tribunal (including decisions as to whether they have jurisdiction) are not subject to appeal and are not liable to be questioned in any court.[80] It is unsatisfactory to exclude the ordinary courts wholly from the review process in the field of the criminal investigations. It has been argued that:

> While [the Tribunal] jurisdiction may be comprehensive, its efficacy as a check and balance on those exercising investigatory powers is limited by a number of factors. First, the absence of any disclosure obligation means that the majority of interferences with privacy will be undetected. In most cases, an individual will only discover that he or she has been the subject of interception or surveillance if criminal proceedings ensue. Secondly, the secrecy surrounding Tribunal proceedings impedes the ability of complainants to present an effective case. Finally, the lack of any appeal process denies an opportunity for potential deficiencies in the initial hearing to be remedied at a later stage. The impact of these limitations is perhaps reflected in the fact that neither the Tribunal nor its predecessors have upheld a single complaint.[81]

It has been argued that that the power to limit or prevent cross-examination, or exclude the applicant or his legal representative, or limit disclosure of evidence may not satisfy the requirements of Article 6 of the Convention.[82] Furthermore, the Secretary of State's power to allocate, by order, proceedings to the tribunal under section 65(2)(d) may impair the

---

[75] Akdeniz, Y., Walker, C. and Taylor, N., 'Regulation of Investigatory Powers Act 2000' [2001] *Criminal Law Review* 73 at 90.
[76] Section 58(2)-(7) of the Act.
[77] Fenwick, H., *Civil Liberties and Human Rights* (London: Cavendish Publishing Limited, 2002) at 718.
[78] Section 68(4) of the Act.
[79] Fenwick, H., 'Covert Surveillance under the Regulation Investigatory Powers Act 2000, Part II' (2001) 65 *Journal of Criminal Law* 521 at 531.
[80] Section 67(8) of the Act.
[81] Ferguson, G. and Wadham, J., 'Privacy and surveillance: A Review of the Regulation of the Investigatory Powers Act 2000' [2003] *European Human Rights Law Review* 101-108.
[82] Fenwick, H., *Civil Liberties and Human Rights* (London: Cavendish Publishing Limited, 2002) at 719-724.

Tribunal's effectiveness and its independence to the point where it no longer meets the requirements of Article 13 of the European Convention.[83] The parliamentary oversight process is limited since "no Committee is directly charged with monitoring State surveillance".[84]

3. The Updated Regime: The Investigatory Powers Act 2016

The Act received Royal Assent on 29 November 2016. The Government introduced legislation to replace the emergency legislation passed in July 2014, the Data Retention and Investigatory Powers Act 2014 (DRIPA), which was subject to a sunset clause providing for DRIPA to be repealed on 31 December 2016. DRIPA replaced the Data Retention (EC Directive) Regulations 2009 (S.I. 2009/859), following the European Court of Justice judgment of April 2014 in the Digital Rights Ireland case, which declared the Data Retention Directive invalid. During the passage of DRIPA, the Government committed to bring forward new legislation which would provide the security and intelligence agencies, law enforcement and other public authorities with the investigatory powers necessary to address evolving threats within a changing communications environment. The Act updates the legal framework governing the state's ability to acquire communications and data about communications. The Act also consolidates and updates powers available to the state to obtain communications and communications data which were previously provided for in a number of different statutes, many of which were enacted before the internet became a widely-used means of communication.

Section 1 of the 2016 provides an overview of the Act, and this section lists offences elsewhere in statute, beyond those in the Act, that provide relevant privacy protections for the powers contained in the Act. This section sets out the numerous duties and considerations to which public authorities must have regard when taking decisions regarding the exercise functions under the Act, including whether to issue warrants, grant authorizations or give notices. Subsection (2) makes clear that when taking such decisions the public authority must consider whether what is sought to be achieved could reasonably be achieved by less intrusive means. The public authority must also have regard to the public interest in the protection of privacy and the integrity and security of telecommunication systems and any other aspect of the public interest in the protection of privacy. It requires that a public authority exercising functions under the Act must have regard to whether the level of protection to be applied to information should be higher because of the particular sensitivity of that information. Applying a higher level of protection in relation to obtaining information will include both considering whether particular safeguards should be applied and taking the sensitivity of the information into

[83] See *Chahal v UK* (1997) 23 EHRR 413; Fenwick, H 'Covert Surveillance under the Regulation Investigatory Powers Act 2000, Part II' (2001) 65 *Journal of Criminal Law* 521 at 535.
[84] Fenwick, H., *Civil Liberties and Human Rights* (London: Cavendish Publishing Limited, 2002) at 678.

account when considering whether obtaining the information is proportionate. Subsection (5) includes examples of sensitive information, including items subject to legal privilege and information that identifies or confirms the identity of a source of journalistic information. Subsection (3) makes clear that public authorities must also have regard to other considerations that are relevant in the context. This section does not list all of the considerations that may be relevant (as this will depend on the context of the particular decision) but lists some of the considerations, including the requirements of the Human Rights Act 1998.

This section does not provide that the public authority must comply with the Human Rights Act 1998 because that is already the case. Subsection (4)(d) does not affect the requirements imposed by the Human Rights Act 1998, including that it is unlawful for a public authority to act in a way that is incompatible with the European Convention on Human Rights. While the title of this section is "General duties in relation to privacy", this does not imply that the requirements of the Human Rights Act 1998 are relevant only where privacy may be interfered with. Which of the Convention rights may be relevant to a decision will depend on the circumstances, but in the context of the use of investigatory powers, Article 8 (Right to respect for private and family life), Article 10 (Freedom of expression) and Article 1 of the First Protocol (Protection of property) are most likely to be relevant.

3.1. Interception of the telecommunications

Section 3 of the 2016 Act deals with the offence of unlawful interception. Subsection (1) makes it an offence to intentionally intercept, in the United Kingdom, a communication in the course of its transmission without lawful authority. This applies to communications in the course of transmission via a public telecommunications system, a private telecommunications system or a public postal service. This offence previously existed under RIPA. Subsection (2) provides that the criminal offence in subsection (1) does not apply where a person has the right to control the operation or use of the system or has the express or implied consent of such a person to carry out the interception. This is relevant to computer networks in the home or workplace for example. Subsections (3), (4) and (5) signpost the sections of the Act which define:

a. interception and when this is understood to be taking place in the UK;
b. public telecommunications system, private telecommunications system and public postal service; and
c. when a person has lawful authority to carry out interception.

A public telecommunications system is a system used to provide a telecommunications service to the public in the United Kingdom. A private telecommunications system is one that is separate from, but connected to a public telecommunications system. This includes

computer networks in the home or workplace. Subsection (6) sets out the penalties for a person who is found guilty of the offence of unlawful interception under subsection (1). The penalty for unlawful interception replicates the penalty which existed under RIPA. No one can be prosecuted under this section except with the consent of the Director of Public Prosecutions in England and Wales or the Director of Public Prosecutions for Northern Ireland in Northern Ireland.

Section 4 of the 2016 Act defines interception and sets out when interception is regarded as taking place in the United Kingdom. Subsections (1) to (5) set out what constitutes intercepting a communication in the course of its transmission by a telecommunications system. There are three elements. Firstly the person must perform a "relevant act", which is defined in subsection (2) and includes modifying or interfering with the system. Secondly, the consequence of the relevant act must be to make the content of the communication available to a person who is not the sender or intended recipient. Thirdly, the content must be made available at a "relevant time", which means a time while the communication is being transmitted or any time when the communication is stored in or by the system. The definition of a relevant time makes it clear that interception includes obtaining stored communications, such as messages stored on phones, tablets and other individual devices whether before or after they are sent. An email which has been sent and is stored on an email server or a voicemail message which has been stored on a telecommunications system to be retrieved later. This would also include an email which had not been sent by an individual but was stored on a server. Section 125(3) of the Postal Services Act 2000 explains that a postal packet is in the course of transmission from the time it is posted to the time it is delivered to the person to whom it was addressed. The same rule applies in this Act.

Section 5 of the 2016 Act sets out conduct that does not constitute interception. Subsection (1) makes clear that interception of a communication broadcast for general reception is not interception for the purposes of this Act. That means, for example, that watching television is not interception. Subsection (2) excludes certain conduct in relation to postal data attached to the communication, e.g. reading the address on the outside of a letter in order to ensure it is delivered to the appropriate location. Section 6 sets out the circumstances in which a person has lawful authority to carry out interception, so the offence of unlawful interception is not committed. There are three ways in which a person may have lawful authority to carry out interception. The first is through a targeted or bulk warrant. The second is through any of the other forms of lawful interception provided for in sections 44 to 52 of the Act, such as interception in prisons or interception with consent. Thirdly, in relation to stored communications, interception is lawful if authorized by an equipment interference warrant or if it is in exercise of any statutory power for the purpose of obtaining information or taking possession of any document or other property or in accordance with a court order. This section also provides that interception or any other conduct authorized

by a warrant under Part 2, a warrant under Chapter 1 of Part 6, or sections 44-52 of the Act is lawful for all purposes. This means that in complying with the authorizations and provisions listed above, a relevant authority or operator is not at risk of being found to be in breach of any other legal requirement.

The Investigatory Powers Commissioner (IPC) has the power to impose fines (via a monetary penalty notice) where unlawful interception has taken place but where the person responsible was not intending to intercept a communication pursuant to Section 7 of the 2016 Act. The Investigatory Powers Commissioner may serve a monetary penalty notice on a person if conditions A and B are met. Condition A is that the Commissioner considers that the person has intercepted, in the United Kingdom, any communication in the course of its transmission by means of a public telecommunication system, the person did not have lawful authority to carry out the interception, and the person was not, at the time of the interception, making an attempt to act in accordance with an interception warrant which might, in the opinion of the Commissioner, explain the interception. Condition B is that the Commissioner does not consider that the person has committed an offence under section 3(1). Section 8 provides a right of redress through the civil courts for the sender or intended recipient of a communication in certain circumstances. The cause of action arises where a communication is intercepted, without lawful authority, in the course of its transmission by means of a private telecommunication system or by means of a public telecommunication system to or from apparatus that is part of a private telecommunication system. Section 9 provides that if a person in the UK asks the authorities of another country or territory to carry out the interception of communications of an individual believed to be in the British Islands at the time of the interception, a warrant authorized under Chapter 1 of Part 2 must always be in place. According to section 10 of the 2016 Act a mutual assistance warrant authorized under Chapter 1 of Part 2 must be in place before a request for interception can be made to authorities outside the UK under an EU mutual assistance instrument or an international mutual assistance agreement. Subsection (3) sets out the meaning of "international mutual assistance agreement" and "EU mutual assistance instrument", which must be designated in regulations made by the Secretary of State.

3.2. Offence of unlawfully obtaining communications data

Section 11 creates the offence of knowingly or recklessly obtaining communications data from a telecommunications or postal operator without lawful authority. The offence may be committed by a person within a public authority with powers to acquire communications data under Part 3 of the Act. It is a defense if a person in a public authority can show that they acted in the reasonable belief that they had lawful authority to obtain the communications data. Section 12 and Schedule 2 restrict general information gathering powers and certain specific pieces of legislation from being used to acquire communications data from a telecommunications or postal operator without the consent of

the operator. Numerous pieces of legislation provide public authorities with powers to require information in certain circumstances. This section ensures those pieces of legislation will no longer be able to be used to acquire communications data from telecommunications or postal operators. This section does not apply where the power specifically relates to telecommunications or postal operators and is exercisable in connection with the regulation of such operators. This is to allow Ofcom and the Information Commissioner's Office to carry out legitimate regulatory functions, such as ensuring the radio spectrum is used in an effective way. These powers can only be used in such a way if it is not possible for the regulator to use the powers in the Act. The restrictions in this section also do not apply where a power is being used to acquire communications data in relation to the conveyance or expected conveyance of any postal item into or out of the United Kingdom. Again, separate powers should only be used if it is not possible for the powers in the Act to be used. Schedule 2 lists the powers that are being repealed or modified. Schedule 2 repeals certain powers so far as they enable public authorities to secure the disclosure by a telecommunications operator of communications data without the consent of the operator.

3.3. Lawful interception of communications

Section 15 deals with interception and examination with a warrant. Subsection (1) explains that there are three types of warrants which can be issued under this chapter: a targeted interception warrant, a targeted examination warrant and a mutual assistance warrant. Subsection (2) describes a targeted interception warrant and provides that such an interception warrant may authorize any activity for obtaining secondary data. Subsection (3) explains that a targeted examination warrant authorizes the examination of material that has been collected under a bulk interception warrant. A targeted examination warrant must be sought 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. Subsection (4) describes a mutual assistance warrant. Such a warrant gives effect to an incoming request, or authorizes an outgoing request, for assistance in relation to the interception of communications. Such a request may be made in accordance with the EU Mutual Legal Assistance Convention, or another international agreement designated in regulations made by the Secretary of State. Subsection (5) confirms that a warrant authorizes any conduct necessary to fulfill what is authorized or required by the warrant, including the interception of communications not specifically described in the warrant, or the obtaining of secondary data from such communications. For example, a warrant can authorize the interception of communications of other individuals who may use the phone line or email account subject to a warrant. A warrant needs to be able to authorize this conduct because it would not be possible to intercept only those

communications belonging to the person that is subject to the interception warrant where other people use the same device.

Section 17 of the 2016 Act sets out the permitted subject matter of a warrant under this Act. Subsection (1) sets out that a warrant under this Chapter may relate to a particular person or organization, or a single set of premises. Subsection (2) provides that a warrant may also relate to a group of linked persons, or to more than one person or organization, or set of premises in the context of a single investigation or operation. A warrant may also relate to testing or training activities, explained in more detail in subsection (3). Section 18 lists those persons who may apply to the Secretary of State for an interception warrant. These are the heads of: the three intelligence agencies; the National Crime Agency (NCA); the Metropolitan Police; the Police Services of Northern Ireland and Scotland; and HM Revenue & Customs, and the Chief of Defense Intelligence. A competent authority of another country may also apply for a mutual assistance warrant. Section 19 sets out the circumstances in which the Secretary of State has power to issue a Part 2 warrant. Subsections (1), (2) and (3) require that the Secretary of State considers that the targeted interception, mutual assistance or examination warrant is necessary (for the purposes set out in section 20) and proportionate to what is sought to be achieved. The decision of the Secretary of State to issue the warrant must then be approved by a Judicial Commissioner before the warrant can be issued. Subsection (4) makes clear that the Secretary of State may not issue a warrant under this section if it relates to serious crime activity in Scotland. In such circumstances the warrant will be issued by the Scottish Ministers. The grounds on which a warrant may be issued by the Secretary of State are set out in section 20. These grounds are: 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. 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. Subsections (5) and (6) specify circumstances in which a warrant may not be considered necessary. 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.

Section 23 sets out the test that the Judicial Commissioner must apply when considering whether to approve a decision to issue a warrant. He or she must review the conclusions the Secretary of State (or the Scottish Ministers) came to regarding the necessity and proportionality of the warrant. In doing so the Judicial Commissioner must apply the same principles that a court would apply on an application for judicial review. The Judicial Commissioner must review the conclusions as to necessity and proportionality with sufficient care to comply with the general privacy duties set out in section 2. Subsection

(4) makes clear that where a Commissioner refuses to approve a warrant he or she must set out written reasons for the refusal. This may allow the agency requesting the warrant to reconsider their application and what action they are seeking to take in order to meet any concerns expressed by the Commissioner. Subsection (5) sets out that the person who issued the warrant may ask the Investigatory Powers Commissioner to reconsider an application that a Judicial Commissioner has refused. Should the Investigatory Powers Commissioner also refuse to approve the warrant there is no right of appeal and the warrant cannot be issued.

3.4 Other Forms of Lawful Interception

There are other forms of lawful interception:

1- Interception with the consent of the sender or recipient: Communications may be intercepted if both the person sending the communication and the intended recipient of the communication have given consent for the interception to take place. The interception of a communication is authorized if either the sender or the intended recipient has consented and surveillance has been authorized.[85]

2- Interception by providers of postal or telecommunications services: Section 45 authorizes interception where it takes place for the purpose of providing or operating a postal service or telecommunications service, of enforcing any enactment relating to the use of such a service, or of the provision of services aimed at restricting access to the content of communications. For example, a postal provider may need to open a postal item to determine the address of the sender because the recipient's address is unknown. A further example is where a telecommunications operator is delivering a service to its customers and the customer has requested that harmful, illegal or adult content is filtered. Subsection (3) makes clear that a telecommunications operator can undertake activity to protect the telecommunication system through which their service is provided and any apparatus attached to that system, to maintain the integrity of their services and to ensure the security of their customers.

3- Interception by businesses etc. for monitoring and record-keeping purposes: Section 46 allows the Secretary of State to make regulations which authorize interception where it would constitute a legitimate practice that is reasonably required for the carrying out of the activities of a business, a government department or public authority. For example, the recording of telephone conversations by businesses, such as call centers, for training or quality control purposes.

[85] Section 44 of the 2016 Act.

4- Postal services: interception for enforcement purposes: Section 47 provides that the interception of postal items is authorized where it is carried out by HM Revenue & Customs in exercising the power in section 159 of the Customs and Excise Act 1979, or by an examining officer under paragraph 9 of Schedule 7 of the Terrorism Act 2000.

5- Interception by Ofcom in connection with wireless telegraphy: Section 48 allows the interception of communications if carried out by the Office of Communications (Ofcom) in the exercise of certain of its functions, including the granting of wireless telegraphy licenses and preventing and detecting interference with wireless telegraphy. Ofcom use equipment to find the source of radio frequency interference rather than to listen to or read communications.

6- Interception in prisons: Prison rules provide a power to intercept communications in prisons in certain circumstances. This section provides that such interception is lawful if it is carried out in accordance with the prison rules. Section 49 does not set out the circumstances in which such interception may be carried out or the safeguards that apply as that detail is contained in the prison rules.

7- Interception in psychiatric hospitals etc. Interception may be carried out in certain psychiatric hospitals if it is in accordance with a direction given under certain other legislation, or in exercise of a power provided in certain other legislation. Section 50 provides that such interception is lawful if is carried out in accordance with the direction or statutory power. This section does not set out the circumstances in which such interception may be carried out or the safeguards that apply as that detail is contained in the relevant direction or legislation.

8- Interception in immigration detention facilities: Certain statutory rules contain powers to intercept communications in immigration detention facilities. Section 51 provides that such interception is lawful if carried out in accordance with those rules. This section does not set out the circumstances in which such interception may be carried out or the safeguards that apply as that detail is contained in the rules.

9- Interception in accordance with overseas requests: Section 52 deals with the issue of interception when a request is made from overseas. Subsections (2) to (5) set out the conditions which need to be met in order that a telecommunications or postal operator may intercept the communications of an individual, at the request of another country. This includes that the individual about whom information is being sought is outside the UK or that the person making the request and the person carrying out the interception believe that the individual is outside of the UK. Further conditions may be contained in regulations made by the Secretary of State.

3.5 Bulk Warrants

The 2016 Act draws a distinction between targeted warrants and bulk warrants. A bulk interception warrant under Chapter 1 of Part 6 (section 138), or a bulk acquisition warrant for communications data (which excludes "content") under Chapter 2 of Part 6 (section 158), or a bulk equipment interference warrant under Chapter 3 of Part 6 (section 178) has to be necessary at least in the interests of national security (but may also be for the purpose of preventing or detecting serious crime or in the interests of the economic well-being of the UK insofar as those interests are also relevant to national security). All three types of bulk warrant under Part 6 of the 2016 Act authorize (among other things) the selection for examination of the data to which they relate and disclosure of such material to the person named in the warrant or to any person acting on his behalf. Bulk warrants are not available to public authorities generally such as the police. An application for a bulk warrant must be made by or on behalf of the head of an intelligence service under sections 138(1), section 158(1) and section 178(1). [86]

The power to issue a warrant must be exercised by the Secretary of State personally under section 141, section 160 and section 182 . Each type of bulk warrant must specify the "operational purposes" for which any material obtained under that warrant may be selected for examination.[87] There are detailed provisions about the making of the list of "operational purposes" by the heads of the intelligence services. An operational purpose may be specified in that list only with the approval of the Secretary of State. The list of operational purposes must be provided to the ISC every three months and must be reviewed by the Prime Minister at least once a year.

In deciding whether to issue a bulk warrant the Secretary of State must apply the principles of necessity and proportionality. The issuing of all three types of warrant is subject to prior approval by a JC. The JC must apply the principles of judicial review.[88] An urgent application for a warrant for bulk equipment interference can be made,[89] in which case there is no prior approval by a JC but instead review after the warrant is issued.

One of the most important issues is that the principles of judicial review include for relevant purposes the legality of an interference with a Convention right under section 6(1) of the HRA ; and therefore the JC must consider for himself or herself questions such as whether an interference is justified as being proportionate under Article 8(2) . It was emphasized that does not mean that the experience and opinion of the agencies is not to be given appropriate weight in the assessment of proportionality. That is conventional in human rights cases. Such respect is owed to those who are responsible for the maintenance of national security and the protection of the public in this country for two reasons. The first

[86] See Phoebe Hirst, "Mass surveillance in the age of terror: bulk powers in the Investigatory Powers Act 2016" (2019) 4 European Human Rights Law Review 403-421.
[87] See section 142(3) , section 161(3) and section 183(4).
[88] See sections 140 , 159 and 179.
[89] Sections 180-181.

is "institutional competence": the Secretary of State and the agencies and others concerned have far greater experience of dealing with these issues than a court can possibly have. The second reason is the democratic legitimacy of the Secretary of State, who is accountable to Parliament. All three types of bulk warrant last for six months[90] unless they have already been cancelled or are renewed.[91] Renewal is subject to approval by a JC.

Bulk interception warrants may cover both the "content" of communications and "secondary data". Bulk equipment interference warrants may cover both content and "equipment data", which is similar to "secondary data". These two concepts are similar to each other and include both "systems data" and in addition "identifying data" which is capable of being separated logically from the remainder of a communication without revealing the meaning of any of the communication. In the case of both bulk interception warrants and bulk equipment interference warrants, their "main purpose" must be to obtain "overseas-related communications", that is communications sent to or received by individuals outside the British Islands or also (in the case of bulk equipment interference warrants) overseas-related information or equipment data. The warrant may also authorise incidental conduct, including incidental interception.[92]

In the case of bulk interception warrants and bulk equipment interference warrants the selection for examination of intercepted content or "protected material" is subject to what is known as the "British Islands safeguard".[93] By way of example, section 152(4) states that: "intercepted content may not at any time be selected for examination if –
(a) any criteria used for the selection of the intercepted content for examination are referable to an individual known to be in the British Islands at that time, and
(b) the purpose of using those criteria is to identify the content of communications sent by, or intended for, that individual."

In contrast, bulk acquisition warrants relate to communications data and do not cover "content". Such warrants are not confined to overseas-related communications. Part 7 of the Act deals with bulk personal datasets. Legal professional privilege is governed by specific provisions in the Act.[94] Confidential journalistic material intercepted or obtained under a bulk interception warrant or a bulk equipment interference warrant is governed by sections 154 and 195 . Additional safeguards for such material apply where targeted examination warrants are sought.[95] It is important to note the "general duties" in relation to privacy which are to be found in section 2(2) of the 2016 Act. These duties apply to a

[90] Sections 143 , 162 and 184.
[91] Sections 144 , 163 and 185.
[92] Sections 136 (5) and 176 (5).
[93] Sections 152(3) and (4) and 193(3) and (4).
[94] See sections 153 , 194 and 222-223
[95] See sections 27, 28, 29 , 55 , 113, 114 and 131

"public authority" within the meaning of section 6 of the HRA other than a court or tribunal. It would therefore include the Secretary of State and the IPC but not the IPT. The duties apply where such a public authority is deciding whether to issue, renew or cancel a warrant under Parts 2, 5, 6 or 7; whether to approve such a decision to grant, approve or cancel an authorization under Part 3; or to give a notice under Part 4.

In exercising the specified functions, section 2(2) provides that the public authority "must have regard to" a number of matters which are then listed, including: "(b) whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant, authorization or notice is higher because of the particular sensitivity of that information". Section 2(5) gives examples of sensitive information for these purposes, including "items subject to legal privilege" and "any information identifying or confirming a source of journalistic information". There is one important aspect of the 2016 Act. This concerns the codes of practice which have been made under the Act. Section 241 gives effect to Sch. 7, which concerns those codes of practice. The Secretary of State must issue a code of practice about the exercise of relevant functions conferred by virtue of the Act. Each code must include provision designed to protect the public interest in the confidentiality of sources of journalistic information; and provision about particular considerations applicable to any data which relates to a member of a profession which routinely holds items subject to legal privilege or relevant confidential information.[96]

"Relevant confidential information" includes information which is held in confidence by a member of a profession and consists of "journalistic material", which would be "excluded material" as defined by section 11 of the Police and Criminal Evidence Act 1984 . Para. 4 of Sch. 7 provides that, before issuing a code, the Secretary of State must prepare and publish a draft of that code and consider any representations made about it.[97] In particular, the Secretary of State must consult the IPC.[98] A code can only come into force in accordance with regulations made by the Secretary of State; and a statutory instrument containing such regulations may not be made unless the draft has been laid before, and approved by a resolution of, each House of Parliament.[99] In other words, the affirmative resolution procedure is required. Under para. 6 of Sch. 7 a person must have regard to a code when exercising any functions to which the code relates by para. 6(1). A failure on the part of a person to comply with any provision of the code does not of itself make that person liable to criminal or civil proceedings but a code is admissible in evidence in any such proceedings.[100] A court or tribunal may, in particular, take into account such a failure

[96] See para. 2(1) (a) and (b) of Sch. 7.
[97] See para. 4(1).
[98] See para. 4(2).
[99] See para. 4(4).
[100] See para. 6(2) and (3).

in determining a question in any such proceedings.[101] A "supervisory authority" may take into account such a failure in determining a question which arises.[102] For this purpose "supervisory authority" includes the IPC and the IPT. The European Court of Human Rights has long recognized that instruments such as a code of practice can be part of the overall scheme which renders any interference with a Convention right "in accordance with the law".

It has been argued that the existence of bulk powers demonstrate the growth in surveillance measures. The limitations on privacy in the age of counter-terrorism surveillance require sufficient protection by the rule of law. Whilst measures in IPA are long overdue, the rule of law safeguards are lacking. The result of the Big Brother case appears to demonstrate the European Court Human Rights' satisfaction with safeguards on paper. At first glance, it appears that the UK's safeguards in relation to bulk powers is one of the best. However, beneath the surface, compliance with the rule of law is lacking.[103]

In the area of secret surveillance, data retention, telephone tapping, and covert intelligence gathering, the European Court of Human Rights has always stressed the need for effective safeguards to minimize the risk of abuse. One of those safeguards in the protection of fundamental rights is to have an independent supervisory body, preferably a judge. The Investigatory Powers Act 2016 for the first time in the UK introduces a judicial element to the authorization of secret surveillance measures by way of Judicial Commissioners and the Investigatory Powers Commissioner. It has been argued that these supervisory bodies do not satisfy the requirements for independence and impartiality found within the jurisprudence of the European Convention on Human Rights. Since surveillance becomes more ubiquitous, the European Court of Human Rights confirmed that essential and adequate safeguards must be in place to protect privacy rights as recognized by Article 8 of the European Convention. This can be achieved by ensuring that the authorizing body of surveillance is independent and impartial. It has been argued that the oversight mechanism found within the 2016 Act is not sufficiently independent, and the introduction of the IPC and JC system of surveillance does not maintain the required independence and impartiality the European Court requires. The cumulative effects of appointments, tenure, dismissal, directions/instructions, staffing/resources and the possibility function alteration posed a serious threat to the independence of the IPC/JC system. The strongest argument on the independence of the IPC/JC system is that it lacks independence due to the unnecessary executive and legislature involvement and the lack of institutional separation between the IPC and JC. This lack of institutional separation also raises doubts as to the impartially of the system, which could also subject the JCs to undue pressures. The greatest

[101] See para. 6(4).
[102] See para. 6(5).
[103] Phoebe Hirst, "Mass surveillance in the age of terror: bulk powers in the Investigatory Powers Act 2016" (2019) 4 European Human Rights Law Review 403 at 420-421.

threat to the independence and impartiality of the JC and IPC may not only come from the executive or the legislature, but from themselves. This research also highlighted that not only could the IPC be marking its own homework by way of audit, inspection and investigation, but also by way of being a sitting judge in the Court of Appeal.[104]

4. Judicial Challenge to the Investigatory Powers Act 2016

In R. (on the application of National Council for Civil Liberties (Liberty)) v Secretary of State for the Home Department, [105] the claimant, a civil liberties campaigning organization, sought a declaration of incompatibility with ECHR rights in relation to various "bulk" warrant powers contained in the Investigatory Powers Act 2016. The provisions under challenge concerned "bulk" powers, as opposed to powers directed at particular individuals. They concerned warrants for: bulk interception (Part 6, Chapter 1,); bulk and thematic equipment interference (Part 6, Chapter 3, and Part 5); bulk personal datasets (Part 7) and the bulk acquisition of communications data and retention notices for, and acquisition of, communications data (Part 6, Chapter 2, Part 3 and Part 4). The claimant submitted that those provisions were incompatible with ECHR art.8 and art.10 because they were too wide, being neither necessary in a democratic society nor proportionate.[106]

The High Court of Justice held that Following the judgment in Human Rights Watch Inc. v Secretary of State for the Foreign and Commonwealth Office [2016] 5 WLUK 352, the Investigatory Powers Tribunal (IPT) had not changed its approach to complaints about secret surveillance. Individuals in the UK were not notified that they had been the subject of surveillance by the intelligence and security agencies. In circumstances where the national system did not provide an effective remedy for a person who suspected that they had been subjected to secret surveillance, the individual did not need to demonstrate the existence of any risk that secret surveillance measures had in fact been applied to them. In Big Brother Watch v United Kingdom (58170/13) Times, November 23, 2018, [2018] 9 WLUK 157, the ECtHR had already held that at least some "bulk" powers, particularly for the collection of data by interception warrants, were in principle compatible with the ECHR. The issue in the instant case was whether the 2016 Act had put in place sufficient safeguards against the risk of abuse of such bulk powers. The Act had created a system of supervision through the office of the Investigatory Powers Commissioner (IPC). There was nothing in the judgment in Big Brother Watch which required there to be prior judicial or independent authorization of bearers or selectors and search criteria. On the contrary, the court had rejected the submission that there should be judicial authorization. It required sufficiently robust independent oversight which was provided by the IPC.

---

[104] Matthew White, "The threat to the UK's independent and impartial surveillance oversight comes not just from the outside, but from within" (2019) 5 European Human Rights Law Review 512 at 533.
[105] [2019] EWHC 2057 (Admin); [2019] 7 WLUK 488.
[106] For discussion see: Case Comment: Security and Intelligence (2019) *Public Law* 784.

The ability to effect interception in bulk was a critical capability for the intelligence services so as to protect the public because patterns of activity might be identified which indicated a threat to the UK. The interlocking provisions of the Act contained sufficient safeguards against the risk of abuse of discretionary powers, including the creation of the IPC. Those safeguards were sufficient to meet the ECHR requirement as to the quality of law. The Act was compatible with ECHR rights insofar as the challenge concerned bulk interception warrants; bulk and thematic equipment interference warrants; bulk personal datasets warrants; and warrants for bulk acquisition of communications data and retention notices for, and acquisition of, communications data. Parliament had created a scheme for the grant of warrants in prescribed circumstances which were carefully regulated by the Act and the codes of practice made under it as well as the supervision of the office of the IPC. The issuing of warrants was subject to many safeguards which were sufficient to prevent arbitrary interference with rights under art.8 and art.10. The powers in the Act did not lack sufficient safeguards for lawyer-client communications. The rules regarding legally privileged items were set out with sufficient clarity and safeguards so as to avoid arbitrary interference and render the scheme compatible with art.8.

There were not insufficient safeguards for the protection of confidential journalistic material in the Act, including the confidential sources of a journalist's material. Unlike a situation where surveillance measures were directed at uncovering journalistic sources, there was no requirement either in the Act or the codes of practice for there to be prior judicial or other independent prior authorisation before a warrant could be issued for the selection for examination of journalistic material or confidential journalistic material after it had been obtained under a bulk warrant. In Big Brother Watch, the ECtHR had been invited to state that there was a requirement for such authorization but had declined to do so, and it was therefore inappropriate for the instant court to do so. The provisions of the Act were not incompatible with art.10 insofar as it was suggested that there were inadequate protections for journalistic material. There had been defects in the way in which MI5 had operated its handling procedures over recent years, particularly in relation to the retention of data collected pursuant to warrants. Those defects had caused obvious concern to the IPC. However, it was clear that the IPC was capable of dealing with those issues and was doing so. The matter did not provide a basis for making a declaration of incompatibility in respect of the Act.

In conclusion, The "bulk" surveillance powers contained in the Investigatory Powers Act 2016 were not incompatible with ECHR art.8 and art.10. The Act contained interlocking safeguards against the possible abuse of discretionary power which were sufficient to prevent arbitrary interference with rights under art.8 and art.10.

In R. (on the application of National Council for Civil Liberties (Liberty)) v Secretary of State for the Home Department[107], the claimant human rights charity challenged the compatibility of the Investigatory Powers Act 2016 Pt 4 with EU law. Under section 87(1) of the Investigatory Powers Act 2016 the Secretaries of State had power, if they considered it necessary and proportionate for the purposes set out in section 61(7) of the Act, one of which, in paragraph (b), was "the purpose of preventing or detecting crime or of preventing disorder", to issue a retention notice requiring a telecommunications operator to retain communications data.[108]

The claimant sought judicial review of, inter alia, Part 4 of the 2016 Act, which contained section 87 , on the ground that it was incompatible with European Union law in that (i), in the area of criminal justice, access to retained data was neither limited to the purpose of combating "serious crime" nor subject to prior review by a court or an independent administrative body; (ii) Part 4 provided for the general and indiscriminate retention of data, contrary to article 15 of Parliament and Council Directive 2002/58/EC , read in the light of the Charter of Fundamental Rights of the European Union; and (iii) Part 4 was incompatible with article 15 of the Directive since it applied to "entity data", one of two mutually exclusive categories of communications data defined in section 261 of the 2016 Act, the other being "events data". The Secretaries of State conceded that Part 4 of the 2016 Act was inconsistent with European Union law in the respects alleged in the first ground. Issues arose as to whether the appropriate relief in respect of the conceded inconsistency was to make an order misapplying Part 4 , suspended to allow time for the introduction of legislation which was compatible with European Union law, or to grant a declaration that Part 4 was inconsistent with European Union law to the extent conceded. [109]

On the claim, the Royal Court of Justice (Divisional Court) allowed the claim in part, and held that there was no automatic rule that, where national legislation was held or conceded to be incompatible with directly effective European Union law, the court should make an order that the national legislation be misapplied with immediate effect; that, rather, the crucial factor when determining the appropriate relief would be the exact nature and extent of the incompatibility; that the incompatibility between Part 4 of the Investigatory Powers Act 2016 and European Union law consisted of two failures to have certain safeguards concerning the retention of data, there being nothing in European Union law which

[107] [2018] EWHC 975, [2019] Q.B 481, [2018] 3 W.L.R 1435.
[108] For discussion: Jonathan Morgan, "O Lord make me pure - but not yet": granting time for the amendment of unlawful legislation" (2019) 135 Law Quarterly Review 585-610; Matthew White, "Data retention: serious crime or a serious problem? (2019) Public Law 633-643; Stuart MacLennan and Steve Foster, Case Comment: R. (on the application of Liberty) v Secretary of State for the Home Department and Secretary of State for Foreign and Commonwealth Affairs: Investigatory Powers Act 2016 - data retention - compatibility with EU Law - order of disapplication", (2018) 23(1) Coventry Law Journal 105-113.
[109] Jennifer Cobbe, "Casting the dragnet: communications data retention under the Investigatory Powers Act" (2018) Public Law 10-22.

prohibited a member state from having in place national legislation which permitted the retention of data for the purpose of preventing or detecting crime along the lines of the 2016 Act; that, since the correction of those failures would require amending legislation setting up an alternative scheme, an order for the immediate disapplication of Part 4 of the 2016 Act would cause chaos and damage the public interest; and that, in those circumstances, and in the light of the Government's proposal to introduce amending legislation, the appropriate remedy was to grant a declaration that (i) Part 4 of the 2016 Act was incompatible with fundamental rights in European Union law in that, in the area of criminal justice, access to retained data was not limited to the purpose of combating "serious crime" and was not subject to prior review by a court or an independent administrative body, and (ii) the incompatibility was to be remedied within a reasonable time, which would be by 1 November 2018.

Having regard to its structure and content, Part 4 of the 2016 Act did not require, or even permit, a general and indiscriminate retention of communications data but, rather, required a range of factors to be taken into account and imposed controls to ensure that a decision to serve a retention notice satisfied, inter alia, the tests of necessity in relation to one of the statutory purposes, proportionality and public law principles; and that, accordingly, Part 4 of the 2016 Act was not incompatible with article 15 of Parliament and Council Directive 2002/58/EC on that ground. Both "location data" and "traffic data", as defined in article 2 of the Directive, as amended, and with which article 15 was concerned, fell within the definition of "events data" in section 261(4) of the 2016 Act; that, therefore, since entity data and events data were, by virtue of the definition of "entity data" in section 261(3) , mutually exclusive, entity data included neither location data nor traffic data; and that, accordingly, entity data under the 2016 Act did not fall within the scope of article 15 of the Directive.

5. Conclusion

The Regulation of Investigatory Powers Act 2000 has regulated certain types of surveillance: interceptions of communications, acquisition and disclosure of communications data, covert surveillance, and encryption. The Act was enacted to ensure that law enforcements surveillance activities are compatible with the Human Rights Act 1998. This chapter has examined whether this main objective has been met. The statutory scheme for interception of communications provided by the Regulation of Investigatory Powers Act 2000 is undoubtedly an improvement on the previous statutory regime under the Interception of Communications Act 1985. Furthermore, the creation of a comprehensive statutory framework for covert surveillance is to be welcomed. Although

the Act is a huge step towards full implementation of the principle of legality and provision of remedies for breach of privacy,[110] several fundamental defects and gaps still remain.

The Act falls short of affording an effective protection for privacy. It gives a wide range of public agencies the power to infringe the individuals' privacy in a very unrestricted and intolerable manner regarding their electronic communications in the light of very limited and complex oversight mechanism by the Tribunal and the Commissioner. The 2000 regime failed to provide a single framework to deal with all interception of communications in the United Kingdom regardless of the means of communications as has been suggested by the Home Office Consultation Paper on the Interception of Communication in 1999. It does not deal with all relevant forms of interceptions especially those carried out by foreign agencies within the United Kingdom or targeted at the United Kingdom. The interception of communications regime under the new legislation has been criticised. It has been argued that:

> Once a warrant has been issued, there is no provision for the subject of an interception authorisation to be informed of the interception after it has taken place. Such a provision, unless in an individual case the disclosure would threaten national security, would make realistically possible for people to protect their rights under Article 8. Just such a disclosure principle is found in Germany's G10 law covering national security surveillance, and was approved by the court in the *Klass* case. In the absence of such a general principle, there is a risk that the Tribunal will be held in Strasbourg not be an effective remedy for the violation of Convention rights under Article 8, leading to a violation of Article 13…the legislation and the Code of Practice on Interception do not offer adequate-or, indeed, any –systemic protection for sensitive communications which, for the purpose of PACE, would fall into the categories of items subject to legal privilege, excluded material, and special material. Recent decisions of the European Court of Human Rights indicate a requirement for a sliding scale of safeguards for privacy rights under ECHR Article 8: the more intimate or confidential information is, the stronger will be the required safeguards if an interference with privacy as to be regarded as being in accordance with the law and proportionate to a legitimate aim. The safeguards in the 2000 Act need to be adjusted to ensure that they take account of this principle.[111]

The Act also does not provide a consolidated and principled legal framework to deal with the sophisticated surveillance techniques and it fails to make the use of covert surveillance by any private citizen a criminal offence. Moreover, the accountability and supervisory mechanism is suffering from serious gaps. It is questionable whether section 17 meets Article 6 requirements since it may not accord with the "equality of arms" doctrine. Although the Codes of Practice, which have been issued by the Secretary of State under section 71 to regulate exercise of the investigatory powers, set out additional safeguards, the value of these safeguards is limited since "the codes have no binding force and there

[110] Feldman, D., *Civil Liberties and Human Rights in England and Wales* (Oxford: Oxford University Press, 2002) at 682.
[111] Feldman, D., *Civil Liberties and Human Rights in England and Wales* (Oxford: Oxford University Press, 2002) at 682-683 (Footnotes omitted).

are no consequences for their disregard".[112] In sum, the Act has struck a fragile balance between national security and privacy demands.

As long as the 2016 Act concerned, it is well established that the supervisory bodies and the oversight mechanism found within the 2016 Act do not satisfy the requirements for independence and impartiality found within the jurisprudence of the European Convention on Human Rights. "The solutions to resolve these problems, or perceived problems, would be to subject the IPC and JC to the same appointment and dismissal system envisaged in the Constitutional Reform Act 2005 and separate by legislation the authorization and review functions of the IPC and JCs. The budget, staffing and resources of the IPC and JC should be determined by an independent body in consultation with the IPC. There should be no ambiguity with regards to the possibility of functionality alterations by the executive. The Prime Minister should not be able to instruct the IPC to conduct additional oversight, as all secret surveillance should already be under their remit. The IPC should be able to publish reports in the public interest without interference from the Prime Minister, even if it is politically damaging. Additionally, judges in the Court of Appeal who are either an IPC or JC should be prevented from sitting on cases revolving around the IPA 2016. That way, the appearance of and actual independence and impartiality of the oversight mechanism is preserved, a measure that is perfectly attainable, and essential in being compliant with the ECHR". Moreover, "the limitations on privacy in the age of counter-terrorism surveillance require sufficient protection by the rule of law. However, national security narratives may stifle expectations as to what the rule of law requires. Recent case law demonstrates that this may even occur in the jurisprudence of European courts. Whilst measures in IPA are long overdue, the rule of law safeguards are lacking. The result of the Big Brother case appears to demonstrate the European Court Human Rights' satisfaction with safeguards on paper. At first glance, it appears that the UK's safeguards in relation to bulk powers is one of the best. However, beneath the surface, compliance with the rule of law is lacking".[113]

[112] Ferguson, G. and Wadham, J., 'Privacy and surveillance: A Review of the Regulation of the Investigatory Powers Act 2000' [2003] *European Human Rights Law Review* 101.
[113] Phoebe Hirst, "Mass surveillance in the age of terror: bulk powers in the Investigatory Powers Act 2016" (2019) 4 European Human Rights Law Review 403 at 420-421.