BigBrother.gov.uk:
State surveillance in the age of information and rights

Yaman Akdeniz, Nick Taylor and Clive Walker*

Citation: Akdeniz, Y.; Taylor, N.; Walker, C., Regulation of Investigatory Powers Act 2000 (1): Bigbrother.gov.uk: State surveillance in the age of information and rights, [2001] *Criminal Law Review*, (February), pp. 73-90.

[PAGE 73 Crim LR]

Abstract

The Regulation of Investigatory Powers Act 2000 signals both the importance of forms of surveillance as techniques of policing and also the human rights apprehensions which those strategies engender. The Act is explained and analysed according to rights-based standards as well as its fit with the development of an "information society".

[PAGE 74 Crim LR]

Introduction

Several deeply-seated factors have tended to impel policing agencies in late modern societies towards techniques of surveillance. One is that information technologies have developed enormously and pervade the economies and societies in western states.[1] Their uses are both for good and ill, the latter being the subject of policing. At the same time, the technologies provide both a new site for policing activity and also furnish a variety of opportunities for surveillance which would not previously have been feasible.[2] The trend

---

* Centre for Criminal Justice Studies, University of Leeds. The authors thank the Police National Legal Database team for their observations.

1 See Akdeniz, Y., Walker, C., and Wall, D., *The Internet, Law and Society* (Longman, London, 2000).

2 See Dandeker, C, *Surveillance, Power and Modernity* (Polity Press, Cambridge, 1990); Lyon, D., *The Electronic Eye: The Rise of Surveillance Society* (Polity Press, Cambridge, 1994); Davies, S., *Big Brother: Britain's Web of Surveillance and the New Technological Order* (Pan, London, 1996); Banisar, D., *Privacy & Human Rights: An International Survey of Privacy Laws and Developments* (EPIC, (Washington DC, 2000).

next represents part of a fundamental switch away from the reactive policing of incidents to the proactive policing and management of risks.[3]

Into the murky world of state surveillance have now been thrust the principles of individual rights in the Human Rights Act 1998, bringing with them much sharper ethical demands in at least two directions.[4] Firstly, there are issues of due process designed to respect human autonomy; if there is to be state surveillance, then it must be delivered "in accordance with the law" and limitations must be precise and accessible.[5] Secondly, there are substantive standards to be observed, including fairness in criminal process (article 6) and respect for individual privacy (article 8). Alongside the ethical emphasis on individual autonomy must be set democratic and legal accountability.[6]

The tasks of recognising and regulating the impetus towards state surveillance in the information age are extraordinarily challenging.[7] Nevertheless, a comprehensive attempt has now appeared as the Regulation of Investigatory Powers Act 2000 ("RIPA").[8] However, whether RIPA adequately addresses the challenges outlined remains doubtful. Certainly, its previous incarnations both as part of what became the Electronic Communications Act 2000 and as the National Criminal Intelligence Service's ("NCIS") Code of Practices were widely seen as failing most rights audits and often failed to pass technical scrutiny. RIPA itself will now be assessed.

Part I : Communications

Part I regulates the interception of communications[9] and follows the proposed reforms briefly outlined in a Home Office Consultation Paper, *Interception of Communications in the United Kingdom* (the "Consultation Paper").[10] Changes were said to be vital because of the advent of the Human Rights Act 1998, as well as the impact of Article 5 of Council Directive 97/66 of 15 December 1997, known as the "Telecommunications Data

---

3 See HMIC, *Policing with Intelligence* (London, 1997/98); JUSTICE, *Under Surveillance* (London, 1998); Policing with Intelligence: Criminal Intelligence: HMIC Thematic Inspection Report on Good Practice 1997/98; Ericson, RV and Haggerty, KD, *Policing the Risk Society* (Clarendon Press, Oxford, 1997).

4 See further Taylor, N., and Walker, C., "Bugs in the System" (1996) 1 *Journal of Civil Liberties* 105; Mohammed, E.A., "An examination of surveillance technology and their implications for privacy and related issues (1999) (2) *Journal of Information, Law & Technology*; Schwartz, P.M., "Privacy and democracy in cyberspace" (1999) 52 *Vanderbilt Law Review* 1609.

5 See *Malone v United Kingdom* App.no. 8691/79, Ser A 82, (1984) 7 EHRR 14.

6 See Marx, G.T., "Undercover" in Fijnault, C., and Marx, G.T., *Undercover – Police Surveillance in Comparative Perspective* (Kluwer, Hague, 1995).

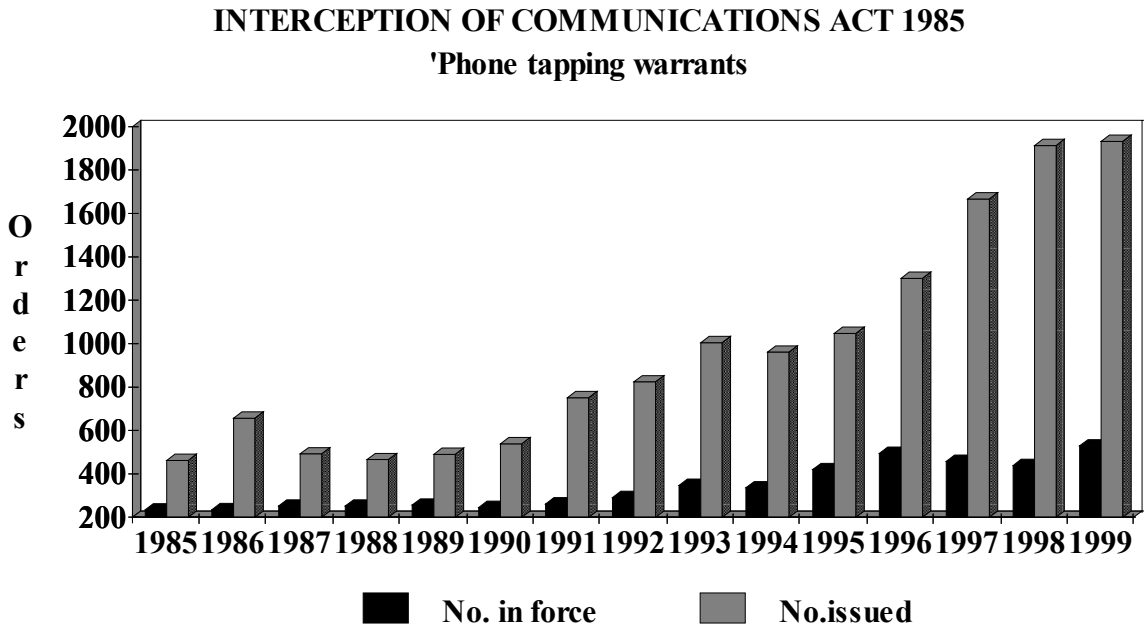
7 See *R v Preston* [1994] 2 AC 130 at pp.145-146 per Lord Mustill.

8 Parts I chapter 1, II and IV are in force, but Part I chapter 2 is expected in mid 2001 and Part III in late 2001.

9 See generally See Lustgarten, L., and Leigh, I., *In from the Cold* (Clarendon Press, Oxford, 1994). A "communication" can include the logging of numbers called: *Morgans v DPP* [2000] 2 WLR 386.

10 Cm.4368. For responses, see http://www.homeoffice.gov.uk/oicd/conslist2.htm, 1999.

Protection Directive".[11] Furthermore, before RIPA, legal controls were very piecemeal, with legislation often responding to adverse or threatening litigation in Strasbourg. A more comprehensive approach was clearly desirable, especially as, new information and communications technologies – [PAGE 75 Crim LR] the Internet,[12] cordless telephones,[13] private exchanges and pay telephones,[14] mobile and satellite telephones and pagers[15] - often did not fit within the existing regulations nor were they necessarily handled by public telecommunications operators with intercept capabilities.[16] In addition, there were allegations of the marked growth in crimes by or against technology, and so interception should take a "crucial role in helping law enforcement agencies".[17] The published statistics do reveal a steady increase in interceptions,[18] but the levels are apparently modest compared to other countries.[19]



11 See further Telecommunications (Data Protection and Privacy) Regulations 1999 SI no.2093. Note also the European Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, Brussels, 12 July 2000, COM(2000)385.

12 See Feather, C., "Interception of email" (http://www.davros.org/legal/interception.html, 1998).

13 *R v W* [1995] 1 AC 309

14 *R v Ahmed* [1995] *Crim. L.R.* 246

15 See *R v Taylor-Sabori* [1999] 1 All ER 160. It is possible that some of these forms of transmissions may still fall outside of RIPA and within the Wireless Telegraphy Act 1949 s.5: Lord Nolan, Report of the Commissioner for 1999: Interception of Communications Act 1985 (Cm.4778, 2000) para.24.

16 For a list, see http://www.oftel.gov.uk/oftlic_c.htm, 2000.

17 Home Office, *Interception of Communications in the United Kingdom* (Cm.4368, 1999) p.i.

18 Source: Lord Nolan, Report of the Commissioner for 1999: Interception of Communications Act 1985 (Cm.4778, 2000) Annex.

19 For example, in the Netherlands, there were 3284 tapping warrants in 1994: Koops, B-J, *The Crypto Controversy* (Kluwer, Hague, 1999) p.76.

Chapter 1: Interception

In order to impose effective regulation upon the interception of communications, section 1 makes it an offence "for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission....".[20] The new regime applies to both public postal and telecommunications systems and also to private telecommunications systems **[PAGE 76 Crim LR]** which are linked to a public network (such as business switchboards).[21] This interception offence is subject to two limitations.

First, if the interception is carried out under section 1(3) with the express or implied consent of a person having the right to control the operation or the use of a private telecommunication system but without lawful authority under RIPA, then it shall be actionable in civil law. But, by section 1(6), conduct is excluded from criminal liability if perpetrated or permitted by the person with a right to control the operation or the use of the system. Second, by section 1(5) the interception has lawful authority under RIPA if it falls within sections 3, 4 or 5 or where an existing statutory power is used in order to obtain stored communications (such a search under warrant or upon arrest under powers in the Police and Criminal Evidence Act 1984).

Section 3 authorises certain kinds of interception where all parties to a communication have consented to the interception (such as the overt use of a telephone answering machine), or where the recipient consents and the communication is subject to surveillance under Part II of RIPA (such as where a kidnapper is telephoning relatives of a hostage) or where the interception arises from necessary conduct in relation to the operation of postal or telegraphy services (such as the opening of an unaddressed letter or counter-measures against interference).

Section 4 provides for various forms of lawful authority:

- One situation (section 4(1)) is where the interception is to be carried out pursuant to regulations relating to an international mutual assistance agreement. This subsection will allow the United Kingdom to comply with Article 12 and 13 of the Convention on Mutual Assistance in Criminal Matters between Member States of the European Union.[22]

Section 4(2) provides for regulations which allow "a legitimate practice reasonably required for the purpose, in connection with the carrying on of any business, of monitoring or keeping a record...".[23] The measure has been implemented by the Telecommunications (Lawful Business Practice) (Interception of Communications)

---

20 "Interception" and "transmission" of communications (but not postal items) are defined in section 2. "Communications" for these purposes do not include "traffic data", since they are regulated by Part 1 chapter 2. The territorial limitation of RIPA is explained by sections 2(4) and 20.

21 This responds to *Halford v UK*, App. no. 20605/92, 1997-III, (1997) 24 EHRR 523; *A v France* App.no. 14838/89, Ser A 277B. It replaces a Home Office Circular 15/1999, Interception of Non-Public telecommunications Networks (1999).

22 Official Journal C 197 (2000), http://europa.eu.int/scadplus/leg/en/lvb/l33108.htm, arts.12, 13. See House of Lords Select Committee on the European Union, 12th Report (1999-00 HL 93)

23 "Business" includes government departments and public authorities: section 4(7).

Regulations 2000,[24] which contain a very broad list of exceptions, including the recording of conversations for contractual and regulatory purposes and the detection of unauthorised use, subject to notification to potential users. Though interference in the lives of employees who utilise the communications equipment of their employers is broadly permitted by Article 5 of the Telecommunications Data Protection Directive, this discretion to snoop randomly and routinely may foster **[PAGE 77 Crim LR]** breaches of article 8 of the European Convention[25] and the Data Protection Act 1998.[26]

- Likewise, under section 4(4) and (5), untrammelled discretion is given to the relevant authorities to intercept the communications of prisoners[27] and high security psychiatric patients.

More explicit lawful authority is provided for in the shape of interception warrants issued by the Home Secretary under section 5. The warrant must be "proportionate" and "necessary":

"(3) ... a warrant is necessary on grounds falling within this subsection if it is necessary-
(a) in the interests 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; or
(d) for the purpose, in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a warrant by virtue of paragraph (b), of giving effect to the provisions of any international mutual assistance agreement.

(5) A warrant shall not be considered necessary on the ground falling within subsection (3)(c) unless the information which it is thought necessary to obtain is information relating to the acts or intentions of persons outside the British Islands."

This wording is very similar to that in the Interception of Communications Act 1985 ("IOCA") (which is repealed), but innovations include the recitation of key Convention language – such as "proportionality" and "necessity". In addition, there are some significant changes to the details of warrants. Under section 8, the warrant may relate either to a named person or to a set of premises, though a warrant must still include one or more schedules describing which communications are to be intercepted (for example, telephone numbers or e-mail addresses), numbers, apparatus or other factors.[28] The previous regime allowed reference only to address or telephone number and, because of the ease of change of modes of communication often necessitated applications for

---

24 2000 SI no.2699. See http://www.dti.gov.uk/cii/lbpintro.htm. Compare OFTEL, Recording Telephone Conversations on Private Networks (London, 1999).

25 See the criticisms of the European Commission Working Party on the Protection of Individuals with respect to the processing of Personal Data, Recommendation 2/99 on the respect of privacy in the context of interception of telecommunications (5005/99/Final, 1999) para.9.

26 See Draft Code Of Practice on the Use of Personal Data in Employer/Employee Relationships, Public Consultation Exercise, http://wood.ccta.gov.uk/dpr/dpdoc.nsf/, 2000.

27 See *R v Owen and Stephen* [1999] 1 WLR 949.

28 But this may be disregarded for the interception of external communications under section 5(6): section 8(5).

amendments to warrants.[29] In addition, section 9 now allows warrants to subsist (subject to renewal) for three months (six months if in the interests of national security or for the purpose of safeguarding the economic well-being).[30] There are also restrictions on the use of intercepted [**PAGE 78 Crim LR**] materials (sections 15 to 18),[31] and the retention of the materials must be shown to be necessary.[32]

Third parties, such as communications service providers, may be required to assist in the interception process under section 11.[33] The person must take all reasonably practicable steps to assist and commits an offence if they fail to do so. As well as these duties in specific cases, section 12 allows the Secretary of State to impose regulations (backed by civil proceedings if need be) for the purpose of securing technical assistance. The prospect of expenditure affecting communications service providers was the subject of much criticism during the passage of the legislation. Aside from the negative image which it creates of the private telecommunications sector becoming the electronic narks of the state, there is also the fear that the expense of providing data access and storage will be significantly expensive[34] and will render UK-based providers uncompetitive in a global market. In response, the government offered two concessions. The first is to set up a Technical Advisory Board comprising both governmental and industry representatives (section 13) which can review and advise on any general regulations[35] and any notices issued to individuals. The second is to pay compensation under section 14.

The new interceptions scheme is undoubtedly an improvement on IOCA, but several substantial defects remain. First, there is concern about the limited judicial oversight.[36] Judicial authorisation is supported by the principles of respect for individual rights and the separation of powers. The suggestion[37] that judges would be inappropriate because of the need for an executive officer to deal with cases of national security and economic well-being is wholly spurious. Most cases now arise from international crime (especially drugs), and so it is disingenuous to construct a system which is reflective of a minority rather than a majority of cases. Furthermore, it is not clear why judges would be unable

---

29 Home Office, *Interception of Communications in the United Kingdom* (Cm.4368, 1999) para.7.6.

30 *Ibid.* para.7.13.

31 See Mirfield, P., "Regulation of Investigatory Powers Act 2000: evidential aspects [2000] *Crim. L. R.* ??.

32 But there are broad exemptions from the wider requirements under the Data Protection Act 1998.

33 Home Office, *Interception of Communications in the United Kingdom* (Cm.4368, 1999) para.5.4.

34 A cost of £46bn was estimated by the British Chamber of Commerce, and Demon Internet has estimated extra running costs of up to 15% (http://www.dispatches.demon.net/pr/1999/pr1999-08-19a.html. 1999). But the Home Office reckons that only around a dozen ISP (out of around 300) will be affected and estimates payments under section 14 as amounting to £20m over three years: http://www.homeoffice.gov.uk/ripa/bcc.htm, http://www.homeoffice.gov.uk/ripa/riapt1.htm, 2000.

35 See Home Office, *Interception of Communications in the United Kingdom* (Cm.4368, 1999) paras.5.5, 5.6. The Secretary of State should also consult with the persons likely to be affected and bodies (such as OFTEL) which have related statutory functions: section 12(9).

36 JUSTICE, *Under Surveillance* (London, 1998) p.21, *Regulation of Investigatory Powers Bill* (London, 2000) para.3.4. Compare *Klass v Germany*, App. no.5029/71, Ser A vol.28, (1980) 2 EHRR 214, *Huvig v France* App.no. 11105/84, Ser A 176B para.33.

37 Home Office, *Interception of Communications in the United Kingdom* (Cm.4368, 1999) para.7.2.

to deal with the sensitive categories mentioned. Both subject-areas fall within the scope of the existing powers to grant judicial warrants under the Official Secrets Act 1911, section 9, and the Official Secrets Act 1989, section 11.

[PAGE 79 Crim LR]

A second issue concerning oversight is that the fact of interception is never revealed at any later time to the subject.[38] This decreases substantially the chances of abuse ever being uncovered.[39] The retrospective review by the Tribunal or Commissioner (described later) is far less likely to spot, or indeed to be alerted to, errors, though this limitation is not of itself a breach of the European Convention.[40]

Thirdly, the criteria used in section 5 are unduly expansive, especially the terms "national security" and economic well-being.[41]. It is admitted that "national security" is well removed from the certainty of an offence and is used to build up intelligence pictures.[42] Even the definition of "serious crime" departs from the version in PACE.[43]

Fourthly, no legislative protection is offered for privileged material,[44] though the draft Code of Practice on Interception does provide some recognition, as well as for medical religious and journalistic materials.[45]

Fifthly, the exceptions to the warrant procedure are too broad, especially those under the Lawful Business Practice Regulations[46] and via participant monitoring.[47]

Sixthly, RIPA does not address all relevant forms of interceptions, such as by foreign agencies either within the UK or targeted at the UK.[48] Conspiracy theorists derive most angst from two shady systems. One is Enfopol, set up under European Union's Third

---

38 See *ibid,* para.1.19; Response from Lord Bassam to open letter by Amnesty International (http://www.homeoffice.gov.uk/oicd/ripam.html. 2000).

39 The UK is the only signatory state to have entered a reservation from the Council of Europe Recommendation on the use of data in the police sector which requires a surveillance target to be notified after the event, unless to do so would prejudice the performance of police tasks. See, JUSTICE, *Under Surveillance* (London, 1998).

40 *Klass v Germany*, *loc. cit.* (para.58.

41 See *Kopp v Switzerland* App.no. 23224/94, 1998-II; *Amann v Switzerland*, App. no. 27798/95, Judgment of 16 February 2000.

42 Interception of Communications Act 1985: Report of the Commissioner for 1998 (Cm.4364, 1999) para.14.

43 See RIPA section 81. This is much the same as the definition given in the Police Act 1997 s.93(4).

44 JUSTICE, *Regulation of Investigatory Powers Bill* (London, 2000) para.4.9.

45 RIPA ss.71, 72. See Home Office, *Interception of Communications in the United Kingdom* (Cm.4368, 1999) para.7.16; http://www.homeoffice.gov.uk/ripa/intofcom.htm, 2000, paras.3.7, 3.11.

46 See *Niemietz v FRG*, App.no. 13710/88, Ser A no.251-B, (1993) 16 E.H.R.R. 97; Singleton, S., "E-mail, surveillance and work" (2000) 164 *Justice of the Peace* 698.

47 JUSTICE, *Regulation of Investigatory Powers Bill* (London, 2000) para.3.8.

48 See *R v Governor of Belmarsh Prison ex p. Martin* [1995] 1 WLR 412.

Pillar; this is not an executive agency but is a forum to encourage police co-operation, including the co-ordination of interceptions across borders.[49] Even more sinister is Echelon, a global electronic eavesdropping operation, orchestrated by the US National Security Agency and including a branch at Menwith Hill near Harrogate.[50] RIPA also fails to consolidate pre-existing codes of **[PAGE 80 Crim LR]** regulation of surveillance; it amends,[51] but does not replace, the Wireless Telegraphy Act 1949 section 5, the Intelligence Services Act 1994, section 5, and the Police Act 1997, Part III.[52]

Finally, there is concern that UK law does not now accord with a pan-European timetable and that compliance costs on UK Communications Service Providers will become unduly onerous. The Internet industry especially has issued dire warnings about being forced to relocate[53] not only out of economic necessity but also to preserve customer privacy against snooping by the Government Technical Assistance Centre (operated in theory by NCIS but located in the Security Service's premises)[54] and allegedly capable of remotely selecting traffic and content on a mass scale.[55]

Chapter 2: Acquisition and disclosure of communications data

The scope of this chapter is explained by section 21, which distinguishes between (i) interceptions of communications, including their contents, in the course of their transmission, which falls under chapter 1, and (ii) conduct involving the obtaining or disclosure of "traffic data" or other information about usage or provision of telecommunications or postal services. Examples of "communications data" include equipment and location details, telephone subscriber details, itemised telephone bill logs, e-mail headers, Internet Protocol addresses, and information on the outside of postal items. Once again, in view of the possible financial costs, compensation may be payable (section 24), but there is no oversight by the Technical Advisory Board.

Data of these kinds may be obtained under section 22(2) where necessary:

"(a) in the interests of national security;
(b) for the purpose of preventing or detecting crime or of preventing disorder;
(c) in the interests of the economic well-being of the United Kingdom;
(d) in the interests of public safety;
(e) for the purpose of protecting public health;

---

49 European Parliament written Question E-1402/98, 1999/C 13/043, C13/32 EN 18 January 1999.

50 See Campbell, D., "Echelon: Interception Capabilities 2000 Report" at http://www.cyber-rights.org/interception/stoa/stoa_cover.htm. But see RIPA s.1(4).

51 RIPA ss.73-75.

52 See Colvin, M., "Part III Police Act 1997" (1999) 149 *New Law Journal* 3111; Uglow, S., "Covert surveillance and the European Convention on Human Rights" [1999] *Crim. L.R.* 287; Home Office, Intrusive Surveillance Code of Practice (http://www.homeoffice.gov.uk/oicd/iscop.htm, 1999).

53 See Khela, B., "The luck of the Irish" (2000) *The Lawyer* 26 June p.28.

54 See (2000) *The Times* 12 June p.4; http://www.homeoffice.gov.uk/oicd/ripam.html, 2000.

55 See Foundation for Information Policy Research, http://www.fipr.org/rip/.

(f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
(g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or
(h) for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State."

It is evident that the grounds are considerably wider than those in section 5, reasons (d) to (h) being extra, but are similar to those in sections 28 and 29 **[PAGE 81 Crim LR]** (described below). Any action taken must be proportionate and necessary (section 23(8)).

Where authorisation is given for obtaining and disclosure of the data, then the operator can be compelled (if necessary by civil proceedings) to provide it, though the issuing authority may decide (for example to maintain secrecy or because of superior technical capabilities) to obtain the data itself (section 22(3)). Authorisation will be in writing and must define the conduct authorised and the data to be obtained; the authorisation remains valid for one month (section 23). The issuing authority under chapter 2 is not the Secretary of State but will be an office holder designated by statutory order within the police, intelligence services, Customs and Excise, Inland Revenue, or any other public authority specified by order.

Once again, RIPA gives clearer, more explicit powers (though just for those agencies listed) than either non-statutory codes issued by NCIS[56] or the system under section 29 of the Data Protection Act 1998,[57] which allows data users to make disclosures if necessary for the prevention or detection of crime or for the purpose of any criminal proceedings by the users (holders) of personal data contrary to the stated restraints on the registered forms of disclosure.[58] RIPA also deals with the privatisation and growth of the telecommunications sector and demands co-operation on a wider basis.[59] On the other hand, encouraged by European Union edicts,[60] it potentially empowers an alarmingly large range of public agencies to snoop, ranging from the Egg Inspectorate to GCHQ, and

---

56 See Code of Practice on the Interception of Communications and Accessing Communications Data (http://www.ncis.co.uk/, 1999). Compare *Valenzuela Contreras v Spain*, App.no. 27671/95, 1998-V.

57 ACPO and ISP Industry, 1999, http:www.linx.net/misc/dpa28-3form.html. There were 18000 such requests by Customs and Excise in the first quarter of 1998: http://www.homeoffice.gov.uk/ripa/commdata.htm, 2000. See Akdeniz, Y., "New Privacy Concerns: ISPs, Crime prevention, and Consumers' Rights," [2000] 14(1) *International Review of Law, Computers and Technology* 55.

58 The system would almost certainly fail under the European Convention standards set out in *Huvig v France* App.no. 11105/84, Ser A 176B; *Kopp v Switzerland* App.no. 23224/94, 1998-II; *Kruslin v France* App.no. 11801/85, Ser A 176A; *Lambert v France* App.no. 23618/94, 1998-V.

59 Home Office, *Interception of Communications in the United Kingdom* (Cm.4368, 1999) para.5.4.

60 Council Regulation on the Lawful Interception of Telecommunications 1995 OJ 96/C/329; Memorandum of Understanding on the Lawful Interception of Communications EU JHA – Council, 25 October 1995.

for a rambling array of reasons.[61] And most serious of all, it allows intervention on the basis of standards and procedures which are intentionally laxer than chapter 1 on the grounds that interception is a much greater intrusion than the collection of traffic data.[62] The Data Protection Commissioner is critical, contending that "access to traffic and billing data should also be made subject to prior judicial scrutiny".[63]

Part II: Surveillance and Covert Human Sources

Part II of RIPA provides a regulatory framework for the use of three types of covert surveillance, namely, directed surveillance, intrusive surveillance and the use [PAGE 82 Crim LR] and conduct of covert human intelligence sources. It was imperative that legislation was provided in these areas to coincide with the increasing use and importance of surveillance as an evidence and intelligence gathering tool, and the commencement of the Human Rights Act.[64] However, even under RIPA there is no requirement on the part of a public authority to obtain an authorisation for covert surveillance, and the decision not to obtain such authorisation does not mean that the action is automatically unlawful. The lack of authorisation would render such actions more vulnerable to challenge under the Human Rights Act, but the nature of surveillance means that it is often unlikely that such operations are uncovered.

Part II begins by drawing a somewhat ambiguous distinction between "directed" and "intrusive" surveillance. The former is surveillance that is covert and undertaken for the purposes of a specific investigation, is likely to result in the obtaining of private information about a person (even though that person may not be specifically identified in relation to the operation), and is not an immediate response to circumstances or events. "Intrusive" surveillance is covert surveillance which is carried out by an individual on residential premises[65] or in any private vehicle or is carried out by a surveillance device in relation to anything taking place on residential premises or in a private vehicle. In this respect it fills the gaps left by the Police Act 1997, Part III, which covers only those devices whose installation require a trespass to property, criminal damage or interference with wireless telegraphy. It is unfortunate, however, that Part III has not been consolidated into RIPA, leaving the law in an inaccessible state.[66] Furthermore, section 26(5) adds that if the device is not actually present on the premises or in the vehicle, the surveillance will not be regarded as intrusive "unless the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle".[67]

---

61 JUSTICE, *Regulation of Investigatory Powers Bill* (London, 2000) para.4.6.

62 Home Office, *Interception of Communications in the United Kingdom* (Cm.4368, 1999) para.10.9.

63 Data Protection Commissioner, Briefing For Parliamentarians on RIP, http://www.fipr.org/rip/DPCparlRIP.htm, 2000.

64 See especially *Govell v United Kingdom* App.no. 27237/95, [1997] EHRLR 438; *Khan v UK*, App. no.35394/97, [2000] *Crim. L.R.* 684, (2000) 5 *Journal of Civil Liberties* ??.

65 See RIPA section 48.

66 See, JUSTICE, *Under Surveillance* (1998) p.19.

67 RIPA s.26(5)(b)

These definitions appear to protect places rather than people, with "intrusion" only occurring if the target is situated in his or her residential property or a vehicle. It would appear to fail to recognise that surveillance that is intrusive may occur outside of these places through, for example, prolonged surveillance, or in a place in which the target would legitimately expect to enjoy privacy.[68] The European Court has recognised the existence of privacy rights beyond the home. For example, in *Niemitz v Germany*,[69] it was held that a person is entitled to a degree of privacy beyond an "inner circle" and as such may include business and professional relationships. The blurring of the boundaries between directed and intrusive surveillance has consequences for the level of authorisation required, as is illustrated **[PAGE 83 Crim LR]** below. According to JUSTICE, the Home Office have stated that directed surveillance being "non-intrusive" is not to be taken too literally.[70] It is non-intrusive only to the extent that it is not "intrusive surveillance" under section 26(3). One could certainly argue that such interpretation precludes the legislation from being "accessible".[71] Moreover, if the Home Office accepts that the level of surveillance beyond residential places or vehicles can be, in fact, intrusive, there would appear no reason why its regulation should be of a lower level than the statutory "intrusive" surveillance. On this basis, the only difference is where it occurs, suggesting that the guiding principle behind the protections under Part II of RIPA is the location of the surveillance rather the effect on the individual.[72]

A further difficulty is raised by section 26(5). If a listening device is used remotely to gather information from inside residential premises, then whether it is directed or intrusive will depend upon its recording capabilities, though the actual invasion of privacy may not be any less. The practical effect is that the capability of the equipment used will determine the extent of the authorisation required rather than the extent and impact of the invasion of privacy (though it is recognised that the issues are linked).[73]

Authorisation of "directed" surveillance is outlined in section 28 and requires only internal authorisation. A designated person may grant authorisation for the carrying out of

---

68 See also Response of the Data Protection Commissioner to the Government's Regulation of Investigatory Powers Bill: A Briefing for Parliamentarians, (http://wood.ccta.gov.uk/dpr/dpdoc.nsf, 2000) para. 10; Covert Surveillance Draft Code of Practice para. 2.7, available at www.homeoffice.gov.uk/ripa. It follows that most CCTV systems fall outside RIPA, despite raising many privacy concerns: Norris, C., Moran, J., and Armstrong, G. (eds.,) *Surveillance, Closed Circuit Television and Social Control* (Ashgate, Aldershot, 1998).

69 *Niemietz v Germany*, *loc. cit.*

70 JUSTICE, *Regulation of Investigatory Powers Bill Human Rights Audit*, Surveillance and Society Seminar Series, University of Hull, 18 April 2000

71 See, *Malone v UK*, *loc. cit.*

72 During the Committee Stage of the Bill it was suggested that intrusive surveillance should, so as to satisfy Article 8, be defined as taking place in circumstances in which a person has a reasonable expectation of privacy. The Minister of State for the Home Office, Charles Clarke stated that such an amendment "would mean ... that the police would have to know before each covert surveillance operation began where their target was likely to go and whether he might find himself in circumstances in which he or another could have a reasonable expectation of privacy". House of Commons Standing Committee F, 30 March 2000.

73 See, Response of the Data Protection Commissioner (2000) para. 11

"directed" surveillance if he believes that it "is proportionate to what is sought to be achieved" and is necessary: in the interests of national security; for the purpose of preventing or detecting crime or of preventing disorder; in the interests of the economic well-being of the United Kingdom; in the interests of public safety; for the purpose of protecting public health; for the purpose of assessing or collecting any tax, duty or levy payable to a Government department; or for any purpose not mentioned above which is specified by an order made by the Secretary of State. Many of these grounds derive from the recognised grounds for interfering with the right to private life under Article 8 of the Convention. The addition of a ground allowing directed surveillance for the purposes of assessing or collecting tax would appear problematic as it is not explicitly encompassed within a ground recognised by Article 8(2). The same can be said in relation to the power vested in the Secretary of State to add to these grounds in section 28(3)(g).

The "designated person" who may grant such authorisation is defined in section 30 as "individuals holding such offices, ranks or positions with relevant public authorities as are prescribed for the purposes of this subsection by an order" made by the Secretary of State and can include the Secretary of State himself.[74] Such relevant public authorities include the police, the intelligence and security services, Customs and Excise, the armed forces and any other authority designated by an **[PAGE 84 Crim LR]** order from the Secretary of State.[75] In small organisations this may lead to authorising officers authorising surveillance activities in operations in which they are directly involved.[76]

The authorisation of "intrusive" surveillance is more narrowly defined. The Secretary of State and "senior authorising officers" have the power to grant authorisation for intrusive surveillance. As with directed surveillance, the issue of proportionality should be addressed (could the information reasonably be obtained by other means) alongside a consideration of whether the authorisation is necessary: in the interests of national security; for the purpose of preventing or detecting serious crime; or in the interests of the economic well-being of the United Kingdom.

The Secretary of State can grant authorisation for intrusive surveillance on an application from the intelligence services, the Ministry of Defence, the armed forces, or a public authority designated as one whose activities may require the use of intrusive surveillance. Senior authorising officers grant authorisations for the police and customs, and they are police Chief Constables (including many non-Home Office forces), and any customs officer designated for the purpose by the Commissioners of Customs and Excise. In cases which may be regarded as urgent an application for authorisation may be made to an Assistant Chief Constable or a designated assistant to the stipulated customs officer.

When authorisation is given or cancelled for intrusive surveillance, be it urgent or non-urgent, notification must be given to the Surveillance Commissioner (described later) as

---

74 RIP (Prescription of Offices, Ranks and Positions) Order 2000 SI no.2417.

75 The public authorities entitled to authorise directed surveillance are listed in Schedule 1 of the Act.

76 Covert Surveillance Draft Code of Practice para. 3.10. See JUSTICE, *Under Surveillance* (London, 1998) p.22.

required under section 35. The Surveillance Commissioner must then decide whether or not to approve the authorisation based on a consideration of the relevant grounds and the issue of proportionality, and if he does so, it shall take effect when the applicant has received written notice. If it is deemed to be urgent, case authorisation takes place immediately it is granted. It is argued, however, that there is no need to dispense with prior judicial approval even in a urgent case. Any intrusive surveillance operation requires a certain level of planning, and one can scarcely imagine a situation when it is impossible to obtain the requisite approval in advance.[77]

If the Surveillance Commissioner is not satisfied that the grounds for authorisation have been met he may cancel the authorisation, or cancel an authorisation with effect from when the relevant grounds ceased to exist to his satisfaction. The Commissioner, it is noted, is not compelled to cancel the authorisation but has the discretion to do so. As a result of exercising his power to cancel, he may also order destruction of any records relating to information obtained by the authorised conduct. A senior authorising officer may appeal to the Chief Surveillance Commissioner against such an order for the destruction of records, and additionally, may appeal against any refusal to approve an authorisation, or decision to quash or cancel an authorisation for the carrying out of intrusive surveillance.

Covert human intelligence sources are placed on a statutory footing for the first time in section 26(7). The necessity for legal regulation in this area was highlighted **[PAGE 85 Crim LR]** in the case of *Texeira de Castro v Portugal*.[78] A person is defined as a covert human intelligence source if he maintains a relationship with a person for the covert purpose of obtaining information or providing access to any information to another person, or covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of the relationship. Authorisation for the conduct or use of covert human intelligence sources is on the same grounds as for directed surveillance, and the persons entitled to grant authorisation are defined as for directed surveillance in section 30.[79] It is arguable whether this level of authorisation is enough to satisfy the European Court. In *Kopp v Switzerland*,[80] the practice of internal authorisation of surveillance activities without judicial authorisation was severely criticised. Thus, certainly in the case of serious crime, internal supervision may not provide a sufficient safeguard.

In summary, Part II of the Act does provide an element of legal accountability in relation to the authorisation of many surveillance operations. It provides a legal framework designed to ensure such activities are "in accordance with law" as required by the Human Rights Act. As has been illustrated above, however, Part II of the Act allows for a considerable amount of detail to be determined through the use of delegated legislation. Such delegation does little for the clarity of the law, which already allows broad

---

77 JUSTICE (*ibid.,* p.21) made the same comment in relation to the Police Act 1997.

78 *Teixeira de Castro v Portugal*, App. no. 25829/94, 1998-IV, (1999) 28 EHRR 101.

79 See further RIP (Source Records) Regulations 2000 SI no.2725.

80 *Kopp v Switzerland* App.no. 23224/94, 1998-II.

discretion and very limited independent oversight. In *Kruslin v France*,[81] the European Court commented, "it is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated". Whether Part II of the Act meets those standards is open to debate.

Part III: Encryption

The explanation behind the introduction Part III of RIPA was that society would suffer if "criminals are able to use such technology without law enforcement having corresponding powers of decryption".[82] The new powers were introduced despite the anxieties over possible human rights infringements. Furthermore, many respondents to the July 1999 consultation paper, *Promoting Electronic Commerce*, raised concerns that government access to keys ("GAK") for decrypting protected data would seriously undermine "e-commerce and the integrity of service providers, as well as causing huge potential costs in global key revocation and change."[83]

Section 49 deals with powers to require disclosure of any protected information where the authorities by notice to the person whom he believes to have possession of the encryption key, impose a disclosure requirement in respect of the protected information under section 49(2). Under section 49(3), a disclosure requirement in respect of any protected information must be necessary:

"(a) in the interests of national security;
(b) for the purpose of preventing or detecting crime; or **[PAGE 86 Crim LR]**
(c) in the interests of the economic well-being of the United Kingdom."

In the case of *Amann v. Switzerland*,[84] the European Court of Human Rights stated that "tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated." This ruling, which condemned wording relating to national security, suggests that section 49(3) above is an inadequately detailed basis for disclosure powers.

Although 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, this intention of protecting the integrity of signature keys, will very often fail since RIPA also allows access to encryption keys. In many cryptographic

---

81 *Kruslin v France* App.no. 11801/85, Ser A 176A, (1990) 12 EHRR 547.

82 DTI, Summary of Responses to "Promoting Electronic Commerce" Consultation on Draft Legislation and the Government's Response to the Trade and Industry Committee's Report (Cm. 4417, 1999).

83 DTI, Promoting Electronic Commerce: Consultation on Draft Legislation and the Government's Response to the Trade and Industry Committee's Report (Cm.4477, 1999) para. 20.

84 App. no. 27798/95, Judgment of 16 February 2000.

products the same passphrase (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.[85] This duality is confirmed in the draft Code of Practice[86] which states "where there are reasonable grounds to believe that a key has been used for electronic signature and, additionally, confidentiality purposes, that key may be required to be disclosed under the terms of the 2000 Act."[87] In practice, this failure to distinguish will undermine the use of digital signatures and hinder the development of e-commerce, conflicting with the intentions of the Electronic Communications Act 2000.

Section 50 deals with the effect of notices imposing disclosure and requires the person who has been served a section 49 notice to convey the information in an intelligible form (under section 50(1)(b)). The provision of any private keys which are capable of decrypting the protected information would also suffice for complying with a section 49 notice under section 50(2)(a). However, under section 50(3), disclosure of any key to the protected information that is in the possession of the person who has been served a section 49 notice at a relevant time could be required if for example the notice states, in pursuance of a direction under section 51, that it can be complied with only by the disclosure of a key to the information as stated in section 50(3)(c). Many critics believe that any form of GAK is very damaging to trust and confidence in the use of public key cryptography.[88] Accordingly, section 51 seeks to limit the situations in which direct access to keys can be required. Under section 51(4), a person[89] shall not give a 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 **[PAGE 87 Crim LR]**
(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 shall include the extent and nature of any protected information, in addition to the protected information in respect of which the disclosure requirement is imposed, to which the key is also a key.[90]

---

85 See DTI, Summary of Responses, *loc. cit.*, para.22.

86 Draft Code of Practice, on Part III of the RIP Bill, Investigation of electronic data protected by encryption etc, 10 July, 2000, at http://www.homeoffice.gov.uk/oicd/ripbill.htm. For an analysis of the Draft Code see Gladman, B., Comments on Draft Home Office Code of Practice on Part III, 11 July, 2000, at http://www.cyber-rights.org/reports/p3copcom.pdf.

87 *Ibid.*, para.8.10.

88 See Cyber-Rights & Cyber-Liberties (UK), "A Critique of Part III, Regulation of Investigatory Powers Bill" (http://www.cyber-rights.org/reports/part-iii.htm, 2000).

89 See RIPA s.51(2), Sched. 2.

90 For a critique, see Gladman, B., "Provisions for Government Access to Keys" (http://www.fipr.org/rip/RIPGAKBG.pdf, 2000), and "Annotated Guide" (http://www.fipr.org/rip/BG_pIIIc.pdf, 2000).

However, the scope of the phrase "special circumstances" in section 51(4)(a) is not legally defined.[91]

Section 52 deals with payments for disclosure. It shall be the duty of the Secretary of State to ensure that appropriate arrangements are in force for requiring or authorising contributions towards the costs incurred by compliance with section 49 notices. Any disclosure will immediately result in the replacement of keys, so payments by the government are inevitable and could (if calculated at true cost) be substantial.

Section 53 deals with a failure to comply with a section 49 notice, A person to whom a section 49 notice has been given will be guilty of an offence (with a maximum penalty of two years' imprisonment) if he knowingly fails to make the disclosure required. Under section 53(2), 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 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. This places the burden of proof on defendants to show that they no longer hold a key that they may previously have held. The presumption of continued ownership is unfair (as contrary to rights concerning the burden of proof and rights against self incrimination under Article 6 of the Convention),[92] since the burden should remain throughout on the prosecution to show that the accused is in a position to provide the key and deliberately refuses to do so.[93] At least section 53 has improved dramatically since it was first introduced within the draft Electronic Communications Bill.[94] In its finalised form, under section 53(3), 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:

[PAGE 88 Crim LR]

"(a) sufficient evidence of that fact is adduced to raise an issue with respect to it; and
(b) the contrary is not proved beyond a reasonable doubt."

---

91 For the draft Code of Practice, on Part III of the RIP Bill, 2000, see Gladman, B., "Comments on Draft Home Office Code of Practice on Part III (http://www.cyber-rights.org/reports/p3copcom.pdf, 2000).

92 See *Funke v France*, App. no. 10828/84, Ser A 256-A; *Salabiaku v France*, App. no.10519/83, Ser A vol.141-A, (1988) 13 EHRR 379; *Murray (John) v UK*., Appl. no. 18731/91, 1996-I, (1996) 22 EHRR 29; *Saunders v UK,* App. no.19187/91, 1996-VI, (1997) 23 EHRR 313; *Serves v. France*, App.no. 20225/92, Reports 1997-VI, (1999) 28 E.H.R.R. 265.

93 This section was first proposed in the Performance and Innovation Unit of the Cabinet Office report, *Encryption and Law Enforcement*, CABI 199-4 278/9905/D16, at http://www.cabinet-office.gov.uk/Innovation/1999/encryption/index.htm, 1999; and was included within the draft Electronic Communications Bill (see DTI's, Promoting Electronic Commerce: Consultation on Draft Legislation and the Government's Response to the Trade and Industry Committee's Report (Cm.4477, 1999)).

94 Clause 10. See generally DTI, Promoting Electronic Commerce: Consultation on Draft, *loc. cit.*, para.4.10.13.

So the defendant does not have to meet a very heavy subsequent responsive burden. Nevertheless, other issues relevant to fairness, such as the nature of the crime, the access to legal advice and the availability of other evidence, remain less settled.

The Government disputed any infringement of Article 6, arguing that the law enforcement agencies would already have the encrypted information and all they need is the encryption key to make the message intelligible:[95]

"We believe that our proposals are ECHR compatible, even when the holder of protected data is required to disclose the key. Of course, the key itself is not self-incriminatory.

In our view, the correct analysis is that a key has an existence independent of the will of the subject. We believe that that was explicitly approved by the European Court in the leading case of *Saunders v. United Kingdom* in 1996. The court found that the right against self-incrimination does not extend to the use in criminal proceedings of material that may be obtained from the accused for the use of compulsory powers, but which has an existence independent of the will of the suspect; for example, documents recovered under a warrant."

Section 54(1) deals with the tipping-off offence (with a five year maximum penalty). A person served with a section 49 notice, or every other person 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. A specific defence to the above tipping-off offence is provided in section 54(5) 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."[96]

Moving from duties placed on the private possessors of the data to the duties placed on the investigative authorities, under section 55(2), it shall be the duty of each of the persons to whom this section applies to ensure:

"(e) that... any key so disclosed is stored, for so long as it is retained, in a secure manner;
(f) 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."

---

95 Lord Bassam, House of Lords Debates, vol.614 col.972, 28 June 2000. Compare Cyber-Rights & Cyber-Liberties (UK), A Further Open Letter to the House of Lords concerning the RIP Bill, http://www.cyber-rights.org/reports/hl-let2.htm, 2000.

96 See Cyber-Rights & Cyber-Liberties (UK), "A Critique of Part III, RIP Bill" at http://www.cyber-rights.org/reports/part-iii.htm, 2000.

Although the Government has accepted that RIPA should include a commitment to the protection of seized keys, there also needs to be a clear commitment to employ the best available methods for key protection. But no guidance either in **[PAGE 89 Crim LR]** RIPA or in the draft Code of Practice[97] is given on the design, development, implementation and operation of the procedures, standards and technical mechanisms needed to provide protection for keys. The fallback is an action in negligence, and the government has agreed that "the duty imposed on public authorities to look after keys should be actionable.".[98] However, there are no criminal offences attached to disclosure of a citizen's data. The conclusions of the Trade and Industry Committee were that "the proposed code of practice may prove to be toothless" and "the impression is given by the legislation that infringements of the code of practice will go unpunished".[99]

Part IV: Scrutiny

The forms of oversight which have existed under IOCA are perpetuated by RIPA. Section 57 provides for the appointment of the Interception of Communications Commissioner to replace the Commissioner appointed under IOCA (currently Lord Justice Swinton Thomas). The Commissioner must keep under review the exercise and performance of the powers and duties under Part I and (in relation to the Secretary of State only) Part III of RIPA. The Commissioner under IOCA has generally been a senior judicial figure, and this pattern is set to continue. The Commissioner must report on any specific defects and must also make an annual report which is laid before Parliament.

The same form of review is extended by section 59 to the powers in sections 5 to 7 of the Intelligence Services Act 1994 (the reviewer being entitled the "Intelligence Services Commissioner"). This appointment replaces the two Commissioners (both posts are currently held by Lord Justice Simon Brown) appointed under the Security Service Act 1989 and the Intelligence Services Act 1994.

The jurisdiction of the Intelligence Services Commissioner does not extend to Northern Ireland (section 59(2)), which is surely open to challenge under articles 8 and 14 of the Convention. On the other hand, there is a special Investigatory Powers Commissioner for Northern Ireland who keeps under review Part II powers (section 60).[100] For England and Wales, the Chief Surveillance Commissioner appointed under Part III of the Police Act 1997 must also now under section 62 of RIPA take on the review of Part II authorisations, Part III activity other than by the Secretary of State and any other areas of RIPA not covered elsewhere. There may also be Assistant Surveillance Commissioners (section 63).

---

97 Draft Code of Practice, on Part III of the RIP Bill, 2000 para.11.9.

98 Per Lord Bassam, House of Lords Debates, vol.615 col.1073, 19 July, 2000.

99 House of Commons Trade and Industry Committee, Fourteenth Report on the Draft Electronic Communications Bill, (1999-00 HC 862) para.34. Note the Government Response, Third Special Report of the Trade and Industry Committee, (1999-00 HC199).

100 See further The Independent Commission on Policing for Northern Ireland), *A New Beginning: Policing in Northern Ireland*. Belfast: Northern Ireland Office, Belfast, 1999.

As well as Commissioners, a Tribunal is established under section 65 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, 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 imposes various restrictions and prohibitions on the disclosure in court of intercepted material and related information); and to hear **[PAGE 90 Crim LR]** and determine any other such proceedings as may be allocated by order. It is emphasised in section 67 that the Tribunal is to exercise merely a form of judicial review. As occurred under IOCA, a Tribunal does not give a straight answer to a complainant but shall simply state whether the determination is favourable or not (thus, not necessarily revealing whether there has been any interception or its details) (section 68).[101]

Most of the criticisms which related to these systems of scrutiny before RIPA remain or are even amplified. Certainly, the structure remains complex, with several different commissioners covering activities which may in fact all be part of the same operation. One wonders whether judicial appointments to the Data Protection Registry would have provided a sounder structure.

The standard of review also fails to inspire confidence. The Tribunal has never found a breach and, because of the rules about non-disclosure, rarely considers cases in which there has been any interception.[102] Though the arrangement is said to be Convention compliant,[103] the cases relied upon[104] are often preliminary Commission decisions. Where similar arguments about the effectiveness of scrutiny in security cases have reached the Court, the applicant has won.[105]

Conclusion

The law has failed to keep pace with the ever more sophisticated surveillance techniques available not just to eager law enforcement agencies but also to possibly unscrupulous private persons. RIPA falls far short of an effective Parliamentary response. The law still does not offer a single legal regulatory system,[106] even though one was promised by the

---

101 See further the Investigatory Powers Tribunal Rules 2000 SI no.2665. The Tribunal replaces those under the Security Service Act 1989 and the Intelligence Services Act 1994, as well as recourse to the Surveillance Commissioners under the Police Act 1997 section 102: RIPA section 70(2).

102 Home Office, *Interception of Communications in the United Kingdom* (Cm.4368, 1999) para.1.9.

103 *Ibid.*, para.2.10.

104 *Christie v United Kingdom*, App. no. 21482/93, 78A D&R; *Esbester v United Kingdom* App.no. 18601/91; *Hewitt and Harman (no.1)* App.no. 12175/86; *Hewitt and Harman (no.2)* App.no. 20317/92; *Redgrave v United Kingdom* App.no. 20271/92; *Preston v UK*, App. no. 24193/94.

105 See *Chahal v UK*, App.no. 22414/93, Reports 1996-V, (1996) 23 EHRR 413; *Tinnelly v UK*, App. nos. 20390/92 ; 21322/93, Reports 1998-IV, (1999) 27 EHRR 249. Compare Special Immigration Appeals Commission Act 1997.

106 JUSTICE, *Under Surveillance* (London, 1998) pp.15, 19.

Home Office.[107] And the law remains weak in terms of the imposition of regulation[108] and the protection for privacy in electronic communications.[109] The statements by the Home Secretary, Jack Straw, under the Human Rights Act that RIPA is Convention compatible and that it is "a significant step forward for the protection of human rights in this country"[110] may eventually be proven to be more the advocacy of a politician than the judgment of a lawyer.

---

107 Home Office, *Interception of Communications in the United Kingdom* (Cm.4368, 1999) paras.4.1, 4.5.

108 Consider here the permissive nature of Part II and also the retention of unspecified residual powers in RIPA section 80.

109 Council of Europe, Recommendation R(99)5, Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways, http://www.coe.fr/dataprotection/elignes.htm, 1999.

110 HC Debs. vol.345 col.767 6 March 2000, Jack Straw.