RESEARCH PAPER 00/25
3 MARCH 2000

The *Regulation of Investigatory Powers Bill*

Bill 64 of 1999-2000

The Regulation of Investigatory Powers Bill creates a framework for the interception of communications, use of surveillance and access to encrypted data by various investigatory agencies. It seeks to ensure that the powers available are used in accordance with human rights. This paper summarises the provisions of the Bill and explores some of the wider issues which it raises.

An earlier version of the proposals on electronic encryption in part III of the Bill was published in the draft Electronic Communications Bill in July 1999. Part II of the Bill (on surveillance and undercover agents) only relates to Scotland in respect of certain reserved powers etc. The rest of the Bill applies to the United Kingdom.

The Bill is due to be considered on Second Reading in the House of Commons on Monday 6 March 2000.

Gabrielle Garton Grimwood

HOME AFFAIRS SECTION

Christopher Barclay

SCIENCE AND ENVIRONMENT SECTION

HOUSE OF COMMONS LIBRARY

Recent Library Research Papers include:

List of 15 most recent RPs

00/10	*Carers and Disabled Children Bill* [Bill 13 of 1999-2000]	01.02.00
00/11	The *Export of Farm Animals Bill* [Bill 20 of 1999-2000]	02.02.00
00/12	The *Armed Forces Discipline Bill* [Bill 53 of 1999-2000]	04.02.00
00/13	The *Northern Ireland Bill* [Bill 61 of 1999-2000]	07.02.00
00/14	The Conflict in Chechnya	07.02.00
00/15	The *Sexual Offences (Amendment) Bill:* 'Age of Consent' and abuse of a position of trust [Bill 55 of 1999-2000]	07.02.00
00/16	*Licensing (Young Persons) Bill* 1999-2000 [Bill 14 of 1999-2000]	09.02.00
00/17	The Parliamentary Oath	14.02.00
00/18	*Postal Services Bill* [Bill 54 of 1999-2000]	11.02.00
00/19	Unemployment by Constituency, January 2000	16.02.00
00/20	European Defence: from Pörtschach to Helsinki	21.02.00
00/21	Economic Indicators	01.03.00
00/22	The *Health Service Commissioners (Amendment) Bill* [Bill 15 of 1999-2000]	01.03.00
00/23	The Criminal Justice (Mode of Trial) (No. 2) Bill [Bill 73 of 1999-2000] **(forthcoming)**	03.03.00
00/24	The National Lottery **(forthcoming)**	03.03.00

Research Papers are available as PDF files:

- *to members of the general public on the Parliamentary web site, URL:* ***http://www.parliament.uk***
- *within Parliament to users of the Parliamentary Intranet, URL:* ***http://hcl1.hclibrary.parliament.u****k*

ISSN 1368-8456

Summary of main points

The Regulation of Investigatory Powers Bill is intended to make provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed.

In the last 15 years there has been a succession of Acts touching on diverse aspects of surveillance and interception of communications; these are described at more length in Part I(A). Until the passing of the *Police Act 1997*, the police's use of electronic surveillance devices ('bugs') on private property - rather than telephone tapping - was subject to Home Office guidelines but not to any statutory regulation. *The Police Act 1997* introduced a Code of Practice on Intrusive Surveillance, which came into force on 22 February 1999. Also introduced in 1999 were non-statutory codes of practice on covert investigatory powers, drawn up by the Association of Chief Police Officers in England and Wales, Association of Chief Police Officers in Scotland and HM Customs and Excise. However, the Government considers that the Codes of Practice may not be enough to protect the police from action under the European Convention on Human Rights.

The case of Halford v United Kingdom at the European Court of Human Rights was a landmark in this area of law. Further impetus for change has come from the *Human Rights Act 1998.*

Part II of this paper describes the provisions of the *Regulation of Investigatory Powers Bill* (except those relating to electronic encryption) and Part IV discusses some of the reactions to the Bill. Interception of communications and other forms of surveillance can be a valuable tool for law enforcement, security and intelligence agencies in tackling serious crime and threats to national security but they also raise some complex and contentious civil liberties and public policy issues - issues which are likely to be debated again in the context of the Bill. There exists a broad spectrum of views on the regulation of investigatory powers. On the one hand, there are those - such as the Police Federation - who believe that the non-statutory Code of Practice on covert investigation is a "handicap on the police". On the other hand, the Foundation for Information Policy Research has argued that the Bill's provisions may infringe citizens' human rights.

Encryption of electronic communications is dealt with in Part III of the Bill and of this paper. The Government's stated aim for this part of the Bill is "to enable law enforcement, security and intelligence agencies to require any person to provide a decryption key or the plain text of specified material in response to the service of a properly authorised written notice". According to the Home Office, "the power would only apply to material which itself has been, or is being, lawfully obtained. There would be strong safeguards and independent oversight to prevent any misuse of these powers. No agency would be able to acquire extra data through the use of this power." [1]

An earlier version of some of these proposals appeared in the consultation before the appearance of the Electronic Communications Bill, but there was some strong opposition to those proposals. Part IV of this paper explains the reasons for that opposition, and discusses whether or not the proposals in the present Bill would be open to the same objections.

---

[1] *Regulation of Investigatory Powers Bill Published Today*: Home Office Press Release 022/2000 10 February 2000

CONTENTS

I Covert investigation: current powers

A. Background

Interception of communications and other forms of surveillance can be a valuable tool for law enforcement, security and intelligence agencies in tackling serious crime and threats to national security. However, the use of interception raises some complex and contentious civil liberties and public policy issues - issues which are likely to be hotly debated again in the context of the *Regulation of Investigatory Powers Bill*.

There is already a body of legislation in this field. Library Research Paper 97/22 described the procedures for authorisation and monitoring which were current up to the introduction of the *Police Act 1997.*[2] A brief chronological summary of the main points of existing legislation is set out below.

The *Interception of Communications Act 1985* was the first Act to regulate the interception by the police and security services (etc) of mail and of telephone calls via the telecommunications network, rather than by the planting of listening devices.

The *Security Service Act 1989* replaced the 1952 Directive from the Home Secretary to the Director-General of the Security Service [the "Maxwell-Fyfe Directive"]. It put the Security Service (MI5) on a statutory footing, defining its functions and management and providing for the issuing of warrants by the Secretary of State for entry on and interference with property. In addition, the Act provided for a Commissioner to review the issuing of warrants and for a Tribunal to consider complaints against the Service.

The main functions of MI5 are defined in the *Security Service Act 1989* as

- *protecting national security*. National security is not defined in the Act, but includes "protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means".
- *safeguarding the economic well-being of the United Kingdom against threats posed by the actions or intentions or persons outside the British Islands.*

Essentially MI5's role is to collect intelligence. In her BBC Dimbleby lecture, Stella Rimington (the then Director-General of the Security Service) said:[3]

---

2 *The Police Bill [Bill 88 of 1996-97]: Intrusive Surveillance:* House of Commons Library Research Paper 97/22

3 *Security and Democracy - Is there a conflict?* - The Richard Dimbleby Lecture 1994, p10

> MI5 has no executive powers, so we pass information on to others and discuss with them what action they can take - to the police, for example, so that arrests can be made; or to the Home Office or the Foreign Office, so that terrorists or intelligence officers can be deported or expelled.

A Home Office circular to the police on the 1989 Act[4] specifically stated that the Act did not "seek to amend the present nature or level of co-operation between the security service and police forces, in particular police Special Branches".[5] Library Research Notes 319 and 423 outlined the background to the debate on the accountability of the Security Service and the 1989 Act respectively.

The *Intelligence Services Act 1994* sought similarly to place the Secret Intelligence Service and the Government Communications Headquarters on a statutory basis. In addition, the Act (as amended) regulated the use by MI5 of bugging devices for the prevention and detection of serious crime, in support of the police and other law enforcement agencies.

The *Security Service Act 1996* (like the *Interception of Communications Act 1985)* endeavoured to define what amounts to serious criminal conduct for the purposes of invoking powers to issue warrants to intercept communications or enter or interfere with property or with wireless telegraphy within the UK or the British Islands.

Until the implementation of the *Police Act 1997*, the powers to carry out intrusive surveillance and interception of communications for the prevention and detection of serious crime were as summarised below:[6]

Agency	**Entry on to/ interference with property**	**Telephone tapping/ postal interception**	**Electronic surveillance ("bugging")**
Police	Governed mainly by the *Police and Criminal Evidence Act 1984*. Some powers to act without a warrant. May apply to a magistrate for a warrant (section 8) or a circuit judge for a production order/ warrant (Schedule 1)	Authorisation by Secretary of State needed (section 2, *Interception of Communications Act 1985)*	Unregulated by statute, but subject to Home Office guidelines. Part III of the *Police Bill* [later *Police Act 1997*] introduced statutory controls
Security Service (MI5)	Authorisation by Secretary of State needed (section 5(3A) & (3B), *Intelligence Services Act 1994*, as amended)	Authorisation by Secretary of State needed (section 2, *Interception of Communications Act 1985*	Authorisation by Secretary of State needed (section 5 (3A) & (3B), *Intelligence Services Act 1994*, as amended)

4 Home Office Circular 89/89: 22 November 1989

5 ibid: para 3

6 This table is based on one which appeared in the *Briefing on the Police Bill 1996* by the civil rights organisation Liberty (November 1996)

Secret Intelligence Service (MI6)	Serious crime: may not take action relating to property in the British Islands (section 5(3), *Intelligence Services Act 1994*, as amended)	Authorisation by Secretary of State needed (section 2, *Interception of Communications Act 1985*	Serious crime: may not take action relating to property in the British Islands (section 5(3), *Intelligence Services Act 1994*, as amended)

As the table demonstrates, until the passing of the *Police Act 1997*, the police's use of electronic surveillance devices ('bugs') on private property - rather than telephone tapping - was subject to Home Office guidelines but not to any statutory regulation. Research Paper 97/22 gives the background to the intrusive surveillance measures in the Act, which caused some controversy when they were debated in Parliament.[7] Liberty, for example, voiced concern that chief constables themselves would authorise intrusive surveillance with no assessment or oversight from courts or Ministers as there would be for analogous police powers or for the MI5's bugging powers in respect of serious crime.[8] Liberty was also concerned at the breadth of both the bugging powers granted to the police and the definition of 'serious crime'. The law lord, Lord Browne-Wilkinson, argued that [9]

> If Parliament enacts, as the Bill proposes, that it be lawful for the police to enter, bug and search our homes, there is nothing that the courts will, in the future, be able to do to protect us from those rights of the state. The bulwark of our freedom will have gone, and not just for the time being but for ever. The powers will be exercisable against us all - the guilty and the innocent alike, in any circumstances which fall within the extraordinarily wide words of the Bill. We will be subject to executive inroads on our freedoms.

The then Government was forced during the passage of the Bill to make concessions on the authorisation procedure. The procedure for authorising surveillance under part III of the *Police Act 1997* (which also applies to HM Customs) is as follows:

- the initial authorisation of an intrusive surveillance operation is the responsibility of the Chief police or customs officer
- prior approval from a Surveillance Commissioner is required, except in urgent cases, if the operation involves intrusion into people's homes, offices or hotel bedrooms, or there are reasonable grounds for thinking that the operation could affect legal, journalistic or confidential personal information (including medical and spiritual counselling)
- in urgent cases Chief Officer authorisations may take effect without prior approval of a Surveillance Commissioner, but the Chief Officer will have to notify a Commissioner as soon as reasonably practicable, giving reasons for proceeding without approval
- a Surveillance Commissioner may approve an operation if he is satisfied that there are reasonable grounds for believing that the action is likely to be of substantial value in the

---

7 *The Police Bill [Bill 88 of 1996-97]: Intrusive Surveillance* House of Commons Library Research Paper 97/22

8 Liberty (formerly the National Council for Civil Liberties) *Briefing on the Police Bill*, November 1996, pp 9-10

9 HL Deb 11 November 1996 Vol 575 Col 797-8 & 801-2

prevention or detection of serious crime and that what the action seeks to achieve could not reasonably be achieved by other means.

Surveillance Commissioners must hold or have held high judicial office. The Prime Minister appointed Sir Andrew Leggatt Chief Surveillance Commissioner on 1 July 1998. There are six Surveillance Commissioners; three for England and Wales, two for Scotland and one for Northern Ireland (although the remit of each Commissioner covers the whole of the United Kingdom so that any Commissioner may act in jurisdictions other than his own). The Commissioners appointed in November 1998 are, for England and Wales, Sir Christopher Staughton (who retired as a Lord Justice of Appeal in December 1997), Sir Michael Hutchison (a retired Lord Justice of Appeal) and Sir Charles McCullough (who retired in January 1998 as the senior judge of the Queen's Bench Division of the High Court). For Scotland the Commissioners are Lord Davidson (who retired in 1996 as a Senator of the College of Justice in Scotland) and Lord Bonomy (a Senator of the College of Justice in Scotland since 1997) and, for Northern Ireland, Sir John MacDermott (who retired in August 1998 as the senior Lord Justice of Appeal in Northern Ireland).

The Secretary of State is required to introduce a Code of Practice on the activities covered by Part III of the *Police Act 1997*.[10] The Code of Practice on Intrusive Surveillance came into force on 22 February 1999.[11] The Code applies to any authorisation of intrusive surveillance (under part III of the Act) by the police, Her Majesty's Customs & Excise, the National Criminal Intelligence Service (NCIS) or the National Crime Squad (NCS). For the purpose of the Code, "intrusive surveillance" means surveillance activity which involves entry on or interference with property or with wireless telegraphy within the meaning of section 92 of the Act. The Code notes that only the Secretary of State in person may authorise the interception of communications sent by post or by means of public telecommunications systems, in accordance with the terms of the *Interception of Communications Act 1985.* Nothing in the code grants any dispensation from the requirements of that Act.

B. The *Human Rights Act 1998*

The *Human Rights Act 1998*, which is already in force in Scotland and will be brought into force in England and Wales and Northern Ireland on 2 October 2000, is intended, as its long title says, to "give further effect to rights and freedoms guaranteed under the European Convention on Human Rights". In particular it will:

- require that, as far as possible, all primary and subordinate legislation is interpreted by the courts and others in a way that makes it compatible with the rights under the Convention;

---

[10] s101, *Police Act 1997*

[11] *Intrusive Surveillance Code Of Practice Pursuant To Section 101(3) Of The Police Act 1997* Home Office 12 February 1999 (available on Home Office website www.homeoffice.gov.uk

- enable courts from the High Court upwards (the High Court of Justiciary in Scotland) to make declarations of incompatibility where they cannot interpret primary legislation in such a way as to make it compatible with the Convention;
- enable the courts to disapply subordinate legislation which cannot be interpreted in a way which makes it compatible with the Convention, unless primary legislation prevents the removal of the incompatibility;
- require all public authorities to act in a way which is compatible with Convention rights. "Public authorities" include courts and tribunals, central government, local government, the police and any other "persons certain of whose functions are functions of a public nature" if the nature of the particular act complained of is not private. It does not include the Houses of Parliament (except the House of Lords in its judicial capacity) or people exercising functions in respect of proceedings in Parliament;
- enable individuals who believe that their rights under the Convention have been breached by a public authority to seek judicial review or to rely on their rights as a defence in civil or criminal proceedings.

The Convention rights protected under the *Human Rights Act 1998* are set out and defined in Schedule 1 of the Act. They are summarised in the titles of the various articles of the Convention as follows:

Article 2	Right to Life
Article 3	Prohibition of Torture
Article 4	Prohibition of Slavery and Forced Labour.
Article 5	Right to Liberty and Security
Article 6	Right to a Fair Trial
Article 7	No Punishment without Law
Article 8	Right to Respect for Private and Family Life
Article 9	Freedom of Thought, Conscience and Religion
Article 10	Freedom of Expression
Article 11	Freedom of Assembly and Association
Article 12	Right to Marry
Article 14	Prohibition of Discrimination[12]

C. The Alison Halford case

The case of Halford v United Kingdom at the European Court of Human Rights was a landmark in this area of law.[13] Ms Halford - formerly Assistant Chief Constable for Merseyside and now AM/AS for Delyn[14] - took her case to the European Court of Human

[12] This means discrimination in the enjoyment of the other rights protected under the Convention. It is not a free-standing anti-discrimination provision

[13] Halford v the United Kingdom (1997) European Court Of Human Rights (73/1996/692/884)

[14] member of the National Assembly for Wales

Rights, arguing that in tapping her personal telephones at work and at home the Chief Constable of Merseyside had infringed her rights under the European Convention.

In May 1983 Ms Halford had been appointed to the rank of Assistant Chief Constable with the Merseyside Police, thus becoming the most senior woman police officer in the United Kingdom at that time. On eight occasions in the next seven years, Ms Halford applied unsuccessfully to be appointed as Deputy Chief Constable in Merseyside and other police authorities. According to Ms Halford, the Home Office consistently withheld its approval for such a promotion, on the recommendation of the Chief Constable of Merseyside Police, who objected to her commitment to equality of treatment for men and women.

Following a further refusal to promote her in February 1990, Ms Halford commenced proceedings on 4 June 1990 in the Industrial Tribunal against, *inter alia*, the Chief Constable of Merseyside and the Home Secretary, claiming that she had been discriminated against on grounds of sex. The eventual hearing before the Industrial Tribunal took place in June 1992.[15] It was in the context of gathering material - specifically, evidence to be used against her - for that industrial tribunal that the alleged breaches took place.

The *Interception of Communications Act 1985* applies to the intentional interception of communications being transmitted by means of a "public" telecommunications system (defined as a telecommunications system which is run pursuant to a licence granted under the *Telecommunications Act 1984* and which has been designated as such by the Secretary of State). Interceptions of calls over private telecommunication systems were therefore outside the scope of the law. As the ECHR noted:[16]

> 26. Sections 2-6 of the 1985 Act *[Interception of Communications Act 1985]* set out detailed rules for the issuing of warrants by the Secretary of State for the interception of communications and the disclosure of intercepted material. Thus, section 2(2) of the 1985 Act provides:
> "The Secretary of State shall not issue a warrant ... unless he considers that the warrant is necessary -
> (a) in the interests of national security;
> (b) for the purpose of preventing or detecting serious crime; or
> (c) for the purposes of safeguarding the economic well-being of the United Kingdom."
> When considering whether it is necessary to issue a warrant, the Secretary of State must take into account whether the information which it is considered necessary to acquire could reasonably be acquired by other means (section 2(2) of the 1985 Act).
> 27. The warrant must specify the person who is authorised to do the interception, and give particulars of the communications to be intercepted, such as the premises from which the communications will be made and the names of the individuals concerned (sections 2(1) and 3 of the 1985 Act).

---

[15] The discrimination case was settled, with an agreement that Ms Halford would take early retirement, receiving a pension and a six-figure lump sum payment

[16] Halford v the United Kingdom (1997) European Court Of Human Rights (73/1996/692/884)

> 28. A warrant cannot be issued unless it is under the hand of the Secretary of State himself or, in an urgent case, under the hand of a senior official where the Secretary of State has expressly authorised the issue of the warrant. A warrant issued under the hand of the Secretary of State is valid for two months; one issued under the hand of an official is only valid for two working days. In defined circumstances, warrants may be modified or renewed (sections 4 and 5 of the 1985 Act).
> …
> 37. The English common law provides no remedy against interception of communications, since it "places no general constraints upon invasions of privacy as such" (Mr Justice Sedley in *Regina v. Broadcasting Complaints Commission ex parte Barclay*, 4 October 1996, unreported).

Article 8 of the Convention provides that:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The Commission agreed that there had been a violation so far as the interception of calls from Ms Halford's office telephones was concerned. It further agreed that, having regard to case-law, telephone calls made from business premises as well as from the home may be covered by the notions of "private life" and "correspondence" within the meaning of Article 8 § 1.

The interception constituted an "interference by a public authority" (within the meaning of Article 8 § 2) with the exercise of Ms Halford's right to respect for her private life and correspondence. Article 8 § 2 further provides that any interference by a public authority with an individual's right to respect for private life and correspondence must be "in accordance with the law". The Court held that the interference was not "in accordance with the law" for the purposes of Article 8 § 2 of the Convention, since the domestic law did not provide adequate protection to Ms Halford against interferences by the police with her right to respect for her private life and correspondence. With no clear evidence, the Court did not, however, find a violation of Article 8 of the Convention with regard to telephone calls made from Ms Halford's home.

Article 13 of the Convention states:

> Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.

The Court recalled that the effect of Article 13 is to require the provision of a remedy at national level, allowing the competent domestic authority both to deal with the substance of the relevant Convention complaint and to grant appropriate relief. The Court concluded that,

given the proven violation of Article 8 of the Convention in relation to the office telephones, Ms Halford was entitled to an effective domestic remedy within the meaning of Article 13. It followed that there had been a violation of Article 13. As regards the home telephones, the Court considered that there was insufficient evidence of an "arguable" claim within the meaning of Article 13 and hence no violation of Article 13.

Article 50 of the Convention provides as follows:

> If the Court finds that a decision or a measure taken by a legal authority or any other authority of a High Contracting Party is completely or partially in conflict with the obligations arising from the ... Convention, and if the internal law of the said Party allows only partial reparation to be made for the consequences of this decision or measure, the decision of the Court shall, if necessary, afford just satisfaction to the injured party.

Taking all relevant matters into account, the Court awarded £10,000 as just and equitable compensation, with £25,000 for costs and default interest at 8% per annum.

The implications of the Halford case attracted much media interest. An article by John Pennycate of the BBC, for example, speculated about the case's implications for people at work.[17]

D. Association of Chief Police Officers' Codes of Practice

For the moment, there are non-statutory Codes of Practice on covert investigatory powers drawn up by the Association of Chief Police Officers in England and Wales, Association of Chief Police Officers in Scotland and HM Customs and Excise. Some of these powers are currently regulated by statute and others not, as explained in Part I of this paper.

The Codes of Practice cover interception of communications, surveillance, use of informants, undercover operations and recording and dissemination. They were published on 13 May 1999, and amended on 12 October 1999, and are available on the NCIS website.[18] They are intended to assist the police by offering examples of good practice - which are already common in many police forces - which will enable them to conduct surveillance operations in a manner consistent with Article 8 of the European Convention on Human Rights. However, the Government considers that the Codes of Practice may not be enough to protect the police from action under the European Convention on Human Rights and hence the Government is bringing forward the *Regulation of Investigatory Powers Bill.*

---

[17] *Watching how you work* by John Pennycate. BBC Online: 20 January 1999

[18] www.ncis.co.uk.

The *Public Statement on Standards in Covert Law Enforcement Techniques* (published with the Codes of Practice) states that

> The principal United Kingdom law enforcement agencies are committed to the maintenance of working practices which observe their obligations under the European Convention on Human Rights.
>
> Those working practices seek to achieve a balance between the requirement to work within a defined framework for the safeguarding of civil liberties and the maintenance of a robust approach to the tackling of crime and criminality.

The Codes have, however, attracted some adverse media and political comment of their own. The following article has been edited for length:[19]

> **European 'human rights' to aid criminals: Police will need permission to watch suspects**
>
> Plain clothes detectives who spot known criminals in the street will need written permission to summon other officers to monitor the suspects' behaviour, under new rules governed by the European Convention on Human Rights.
>
> If the regulations are not followed, any prosecution will automatically fail, even if the officers subsequently witness a blatant crime.
>
> 'This is absolutely potty,' said Ann Widdecombe, the shadow home secretary. 'It shows that all our fears about incorporating the European Convention on Human Rights into British law have been proved right. Jack Straw should state immediately that these rules will not apply here. It is complete nonsense.'
>
> A spokeswoman for the National Crime Squad said the rules would apply from October. 'Under the ECR regulations, if officers are involved in a preplanned surveillance, they will need to obtain written permission as a safeguard for the citizen to ensure that their privacy is not being invaded,' she said.
>
> 'All police officers in this situation will have to get this permission in case their surveillance subsequently results in a person's human rights being infringed. If officers don't get written permission, there is a danger that any conviction would be overturned by the European Court, so these rules are a safeguard for us as well as the suspects.'
>
> The new rules are contained in a Government document on 'standards of covert law enforcement techniques', which has been distributed to police forces across Britain.

---

[19] "European 'Human Rights' to Aid Criminals: Police Will Need Permission to Watch Suspects" *Sunday Telegraph*: 23 January 2000

> One force has summarised the rules by telling its detectives: 'In the scenario where a known shoplifter is seen in shops and plain clothes officers are sent to keep observations, the Superintendent's authority must be sought.
>
> 'In the case, where an officer in plain clothes sees a likely offender, and keeps observations, the authority is not needed. However, if he calls other officers to the scene, a Superintendent's authority is required.
>
> 'These codes will become law in October. If any cases where these codes have been breached are heard after this time, the prosecution will fail.'
>
> Glyn Smythe, the Police Federation's spokesman, said the rules, which have emerged only days after the Government published figures showing a 2.2 per cent rise in crime last year, would make life easier for criminals.
>
> 'The Government is placing another handicap on the police. After the recent rise in crime, Jack Straw has shot himself in the foot again. Officers will be dismayed,' said Mr Smythe.
>
> The Police Federation warned that some surveillances will be delayed as a result of the rules because of difficulties in contacting senior officers to obtain permission. That will increase the risk of crimes being committed.
>
> There will be a further danger that mobile phone calls or radio messages from officers seeking permission to watch suspects will be intercepted by the criminals, alerting them to the police presence. Costs will also be incurred on bureaucracy and phone calls, eating in to police budgets for other operations.
>
> A Home Office spokesman refused to comment on the possible impact of the regulations on the crime figures. He was also unable to explain how plain clothes detectives could infringe 'human rights' by watching what criminals were doing, but said the Government was strongly committed to protecting civil liberties.
>
> 'The Human Rights Act is designed to protect the rights and responsibilities of all citizens and ensure that they are properly recognised,' the spokesman said.
>
> 'In the instance to which you are referring, we need to ensure that we are catching the criminals, but we need to make sure that we are not infringing their civil liberties.'

E. Home Office Consultation paper

In June 1999, the Home Office issued a consultation paper on the interception of communications in the United Kingdom.[20] In this paper, the Home Office set out the Government's proposals for updating the law on interception of communications, to ensure a

[20] *Interception of Communications in the United Kingdom* Cm 4368, also at www.homeoffice.gov.uk

better fit with Article 8 of the European Convention on Human Rights (taking account of the judgement in the *Halford* case), to keep abreast of technological developments in the communications field and to provide

> a single legal framework which deals with all interception of communications in the United Kingdom, regardless of the means of communication, how it is licensed or at which point on the route of the communication it is intercepted.[21]

The executive summary of the consultation paper is reproduced below:

> **Background**
> In most developed countries, interception of communications is used by the law enforcement, security and intelligence agencies in their work against serious crime and threats to national security, including terrorism. The UK is no exception. Interception represents an indispensable means of gathering intelligence against the most sophisticated and ruthless criminals. Its value in the serious crime field is demonstrated by the fact that, in the years 1996 and 1997, lawful interception of communications played a part – often the crucial part – in operations by the police and HM Customs which led to:
>
> - 1200 arrests;
> - the seizure of nearly 3 tonnes of Class A drugs, and 112 tonnes of other drugs, with a combined street value of over £600 million;
> - the seizure of over 450 firearms.
>
> This Consultation Paper sets out the Government's proposals for reforming the legislation which governs the interception of communications in the United Kingdom. The proposed changes are designed to:
>
> (a) update the legislation to take account of communications services introduced since the existing legislation was enacted
> (b) extend the law to cover interception of private telephone networks
> (c) provide a clear, statutory framework for authorising the disclosure of data held by communications service providers
> (d) retain the existing safeguards which ensure that interception is authorised only when it is justified in relation to strict statutory criteria, and that the use of the power is subject to independent judicial oversight.
>
> *The Government intends to introduce legislation as soon as Parliamentary time allows, and invites views on the content of the legislation.*
>
> **Human Rights Act 1998**
> We recognise that, by its nature, interception of communications is a highly intrusive activity, affecting the privacy of the individual. The legal right to respect for a private and family life is established in Article 8 of the European Convention on Human

---

[21] Ibid, para 4.1

Rights (ECHR), which is being incorporated into UK law in the Human Rights Act 1998. The ECHR recognises, however, that there are circumstances in a democratic society where it may be necessary for the state to interfere with this right, but only in accordance with the law and for certain clearly defined purposes. Where such interference does take place, Article 13 ECHR requires a means of redress to be available to the individual. The Government is committed to ensuring that interception of communications complies fully with the ECHR, and this paper describes the separate frameworks for authorisation, oversight and redress with which we propose to achieve this.

This paper deals only with interception of communications. The Government is aware that similar issues arise in relation to other forms of surveillance and the requirements of the ECHR. Many of these issues were addressed in the recent *JUSTICE* report "Under Surveillance". The Government is considering whether changes to current legislation should be extended to cover methods of intrusive surveillance other than interception of communications. Our conclusions will be announced in due course.

The law at present

The Interception of Communications Act 1985 (IOCA) placed interception of communications sent by post or by means of a public telecommunication system on a statutory basis for the first time. The main features of IOCA are summarised below:

(a) The Act created an offence of unlawful interception of communications by post or by means of a public telecommunication system.
(b) It established a framework controlling issue, renewal, modification and cancellation of warrants authorising interception of communications sent by post or by means of a public telecommunication system.
(c) It enshrined in law the principle that warrants may only be issued by the Secretary of State, and specified the purposes for which warrants may be issued as:
  i. in the interests of national security;
  ii. for the purpose of preventing or detecting serious crime; or
  iii. for the purpose of safeguarding the economic well-being of the United Kingdom.
(d) It placed strict safeguards on the extent to which intercepted material may be disclosed, copied and retained, requiring arrangements to be made to ensure that each of these is kept to a minimum.
(e) The Act established an independent oversight regime in the form of the Interception Commissioner, whose job is to keep under review the way in which the power to issue warrants is exercised and the operation of the safeguards described above.
(f) It set up a Tribunal to investigate complaints where the complainant believes that their communications have been intercepted in breach of the Act.

Why is there a need to change the law?

Since the 1985 Act was enacted there have been enormous changes in the telecommunications and postal market, and a great expansion in the nature and range of services available. For example:

- The number of telecommunications companies offering fixed line services has grown from two to around 150.

- Mobile telephones have developed from being virtually unheard of to the mass ownership which is seen today.
- The emergence of totally new services such as international simple resale, which offer cut price telephone calls abroad – there are currently over 200 of these.
- The satellite telephone market, while still in its infancy, will evolve rapidly in the next few years.
- Communications via the Internet have grown dramatically in the last few years, and this part of the market continues to grow.
- The postal sector has also developed rapidly, with a huge growth in the number of companies offering parcel and document delivery services.

The legislation has not kept up with the changes in the communications marketplace; changes which criminals and terrorists have been quick to exploit for their own purposes. If we fail to bring the legislation up to date, we risk degrading the capability of the law enforcement, security and intelligence agencies ("the Agencies").

We also need to update our interception law to encompass private networks**,** which will ensure that the protection currently offered by IOCA to individuals using public telecommunications networks is extended to cover all networks. At present, there is no right of redress in UK law for an individual whose communications have been intercepted if the interception took place on the non-public side of the network. The proposed legislation will make this type of unauthorised interception unlawful, enabling us to give effect to the judgment of the European Court of Human Rights in the case of *Halford v UK*. The law needs to recognise that there are perfectly respectable reasons for allowing employers to record telephone conversations in the work place; for example, in order to provide evidence of commercial transactions or to counter fraud. But the practice needs to be regulated by law, in a way which ensures that the rights of employees are respected in circumstances where they have a reasonable expectation of privacy. The legislation will provide a clear framework governing the interception of private networks, setting out the circumstances in which it may be authorised and the safeguards which should apply.

The Government believes that the law surrounding access to communications data is in need of revision. Itemised billing, for example, can be of tremendous investigative value, and it is right that in certain circumstances the authorities should be able to access this material. However, it also involves a measure of intrusion into individual privacy and it is essential that access should be carefully controlled in accordance with ECHR proportionality requirements, authorisation only being given where necessary and justified for clearly defined purposes. For these reasons we are proposing to establish a clear, statutory framework for access to communications data.

The consultation paper contained a summary of the Government’s legislative proposals:

EXISTING LEGISLATION	PROPOSED CHANGES
IOCA is restricted to interception of communications sent by post or by means of public telecommunication systems	Interception legislation to encompass all communications in the course of their transmission by telecommunications operators or mail delivery systems.
Currently interception warrants specify the address to be intercepted.	Interception warrants to specify a person, and to include a schedule listing all the addresses which the Agency wish to intercept in relation to that person.
Interception warrants may only be issued under the authority of the Secretary of State. Modifications may be made by Senior Civil Servants with the express authorisation of the Secretary of State, or by a person holding office under the Crown, where they have been expressly authorised by the warrant to do so.	The issue of the warrant to continue to be authorised by the Secretary of State. Subsequent modifications to the warrant adding new addresses to be authorised at Senior Civil Service level. Provision to be made allowing urgent modifications with limited lifespan to be made by Head of Agency or nominated deputy who are expressly authorised by the warrant.
Interception warrants are served on the PTO or Post Office, who are required to intercept such communications as are described in the warrant.	Interception warrants to be served on the agency making the application, who will then use it to achieve the interception with reasonable assistance from the Communications Service Provider
All warrants are authorised for an initial period of two months. Thereafter, warrants issued on serious crime grounds are renewed on a monthly basis and those issued on national security or economic well-being grounds are renewed on a six monthly basis.	All warrants to be authorised for an initial period of three months. Warrants to be renewed at three monthly periods (serious crime warrants) and six monthly (national security and economic well-being warrants), bringing them into line with intrusive surveillance provisions.

EXISTING LEGISLATION	PROPOSED CHANGES
There is currently no legislative framework for authorising interception of private (non-public) networks.	Interception on non-public networks to be brought within the scope of the legislation, requiring the Agencies to obtain a warrant before carrying out this type of interception.
There is no legislative framework which addresses recording or monitoring of communications in the course of lawful business practice.	Provision to be made allowing employers to continue recording communications in the course of lawful business practice to provide evidence of commercial transactions or any other business communication, in both the public and private sectors.
Communications data may be supplied voluntarily by holders for specified reasons (eg investigation of crime) under the Data Protection Act and the Telecommunications Act. They may additionally be required to produce it in obedience to a Production Order authorised by a Crown Court judge.	The law regarding provision of communications data for law enforcement, security or intelligence purposes to be amended to require the holder of such data to provide it in response to a properly authorised request.

The areas where no change is proposed

Along with the proposals for change which are contained in the above table and described in detail in this paper, there are several fundamental provisions contained within the Interception of Communications Act which have been unaffected by the developments outlined in the introduction and continue to work well. The Government proposes no change to these provisions, which are listed below:

- There will continue to be an offence of unlawful interception.
- There will be no change to the criteria which must be met before interception of communications may be authorised.
- There will be no change to warrantry procedures authorising interception of external communications.
- The strict safeguards regarding the extent to which intercept material is disclosed or copied will remain, continuing to limit this to the minimum necessary.
- There will continue to be a Tribunal to hear complaints.
- The Interception Commissioner will continue to oversee the use of interception.

In December 1999 the Home Office published an analysis of the responses to the consultation paper. It stated:

> A total of 85 responses were received. This figure does not give a true reflection of the coverage achieved by the consultation since a substantial proportion of the comments received were from representative bodies putting forward the combined views of a large number of their constituents.
>
> The Government is grateful for the responses it has received, which have been carefully considered in the course of preparing the Regulation of Investigatory Powers Bill. The Government intends to introduce this Bill to Parliament shortly. The tenor of the responses was overwhelmingly positive. The vast majority welcomed the opportunity to engage with Government on this issue, and comments were detailed and constructive. Industry in particular welcomed the open nature of the consultation, and many expressed a desire for continuing dialogue.[22]

The responses tend to concentrate on specific points and these are considered in the next part of this paper in connection with the appropriate part of the Bill.

II Regulation of Investigatory Powers Bill (Bill 64 of 1999-2000)

The Bill was presented to the House of Commons for First Reading on 9 February 2000. Launching the Bill, the Home Secretary described the need for new legislation to reflect the changes in the telecommunications industry since the *Interception of Communications Act 1985*:[23]

> The Human Rights Act and rapid change in technology are the twin drivers of the new Bill. None of the law enforcement activities specified in the Bill is new. Covert surveillance by police and other law enforcement officers is as old as policing itself; so too is the use of informants, agents, and undercover officers.
>
> What is new is that for the first time the use of these techniques will be properly regulated by law, and externally supervised, not least to ensure that law enforcement operations are consistent with the duties imposed on public authorities by the European Convention on Human Rights and the Human Rights Act.
>
> Telecommunications interception was only put on a statutory footing at all in the United Kingdom in 1985. But when that Bill was drafted there was one completely dominant provider - BT - with Mercury barely off the ground, and only landlines. No pagers, no mobiles, no e-mail, no internet, no encryption.
>
> The change in the telecom landscape in less than a generation has been revolutionary. We have to ensure that the legislation keeps pace - permitting interception in closely-defined circumstances to protect national security and fight serious crime, whilst resolutely ensuring that citizens' privacy is safeguarded.

---

22 Dep 99/1666, also available on the internet at: http://www.homeoffice.gov.uk/oicd/iocresp.htm

23 *Regulation of Investigatory Powers Bill Published Today*: Home Office Press Release 022/2000 10 February 2000

> This Bill achieves those ends. The passage of this Bill will mark the completion of a twenty-year programme of reform to place police and law enforcement on a properly regulated statutory basis - and the intelligence and security agencies too.
>
> The Police and Criminal Evidence Act 1984, the Security Service Act 1989, the Intelligence Services Act 1994, the Criminal Investigations and Procedure Act 1996, the Police Act 1997, and this Bill, are staging posts on a journey to secure a better balance between law enforcement and individual rights, and proper compliance with the European Court on Human Rights.
>
> Justice for all - victims, accused, and the public - will now be much better served. The old, non-statutory, less formal methods of the past sometimes led to serious miscarriages of justice, dreadful for the individuals concerned, and deeply undermining of public confidence.

General comments on the Bill are set out in part IV of this paper. Detailed commentary on the Bill's provisions can be found in the Explanatory Notes, Bill 64-EN of 1999-2000. The following seeks to highlight some of the most significant areas of the Bill and those which might be most likely to provoke debate but is not an exhaustive summary of the Bill.

A. Part I: Communications: Interception of Communications and the Acquisition and Disclosure of Communications Data

According to the Home Office, Part I of the Bill[24]

- … would bring interception legislation up to date in the light of new developments in communications technology which have occurred since the Interception of Communications Act was passed in 1985; eg e-mail services through Internet Service Providers (ISPs), satellite telephones, and radio pagers, which have developed from being a simple beeper into a means of sending text messages.
- The Bill would also extend the protection provided by interception legislation to non-public networks, eg office switchboards. This is an area not currently regulated, and the proposals would require the Secretary of State to authorise any future state interception on these networks before it can occur.
- There is no change planned to the strict criteria which must be met before an application to intercept can be considered, and each warrant would continue to be personally authorised by the Secretary of State.
- The Bill also proposes that the Secretary of State's power to issue warrants continues to be overseen by the Interception Commissioner - currently Lord Nolan. In order to do this he undertakes inspections of the interception Agencies

---

[24] *Regulation of Investigatory Powers Bill Published Today*: Home Office Press Release 022/2000 10 February 2000

> and relevant Government Departments and makes an annual report to the Prime Minister which is laid before Parliament.

Part I replaces the *Interception of Communications Act 1985*. The Explanatory Notes state that the changes it introduces "go beyond what is strictly required for human rights purposes".[25] The provisions are also intended to implement Article 5 of the EU Telecommunications Data Protection Directive, which requires member states to safeguard the confidentiality of communications.[26]

1. Interception of Communications

Clause 1 makes it an offence for a person intentionally and without lawful authority to intercept, anywhere within the United Kingdom, a communication passing through a public postal service or public or, in certain circumstances, a private telecommunications service. Clause 1 goes beyond section 1 of the *Interception of Communications Act 1985* (IOCA), which the current Bill repeals, by the inclusion of private telecommunications services. A separate and specific civil wrong (tort) of unlawful interception on a private telecommunications network is also created (*subsection (3)*).[27]

Under *subsection (4)* the Secretary of State must ensure that any requests for mutual assistance made under an international agreement on interception of communications, such as the draft EU *Convention on Mutual Assistance in Criminal Matters*, are made with lawful authority. The Explanatory Notes state that in practice this will require the Secretary of State to obtain a warrant under Clause 5 prior to requesting mutual assistance.[28]

Subsection (5) sets out the circumstances in which the offence and tort of unlawful interception do not apply. For example, interception is lawful where a warrant is obtained under Clause 5, where one of the exceptions described in Clauses 3 or 4 apply (see below) or where an existing statutory power is used to obtain stored communications: for example, where a circuit judge orders that stored data relating to messages previously sent to a pager be produced under Schedule 1 to the *Police and Criminal Evidence Act 1984*.

Subsection (6) sets out circumstances in which an interception constitutes a tort but not an offence. The Explanatory Notes state that, essentially, this:

> allows a person with a right to control a private telecommunication network to intercept on their own network without committing an offence. Examples of this type of activity are an individual using a second handset in a house to monitor a telephone

---

25 Bill 64 – EN of 1999-2000, para 8

26 Council Directive 97/66 of 15 December 1997

27 this would give rise to a civil action at the suit of a person who is injured as a result of non-compliance with it.

28 Bill 64 – EN, para 23

> call, and a large company in the financial sector routinely recording calls from the public in order to retain a record of transactions.[29]

Subsection (7) deals with penalties. A person who is found guilty in a Magistrates' Court of the criminal offence of unlawful interception may be fined up to the statutory maximum (currently £5000); in the Crown Court he or she may be imprisoned for a period up to two years, or fined, or both. There is no upper limit to a fine on conviction in the Crown Court.

Clause 2 offers definitions of telecommunications and postal services and systems relevant to the Bill, and contains additional provision on interpretation. The telecommunications definitions etc are intended to be wide enough to anticipate continuing technological advance in the industry and to prevent loopholes which arise under IOCA, such as the interception of a call during its transmission to and from a cordless handset. The Explanatory Notes explain the significance of the definition of the phrase "while being transmitted" contained in *subsection (7)*:

> The times when a communication is taken to be in the course of its transmission include any time when it is stored on the system for the intended recipient to collect or access. This means that an interception takes place, for example, where an electronic mail message stored on a web-based service provider is disclosed to someone other than the sender or intended recipient, or where a pager message waiting to be collected is so disclosed. Provision is made for such disclosures in Clause 1(5)(c).[30]

Clause 3 defines when interception of communications will be authorised by this section of the Bill without need for a warrant, for example, where one of the parties to the communication has consented to its interception *and* it has been authorised by a police officer etc. on one of the grounds contained in Clause 27(3).[31] The Explanatory Notes suggest that this situation might arise where a kidnapper is telephoning relatives of a hostage, and the police wish to record the call for the purpose of preventing or detecting serious crime.[32] This provision may go some way to meeting the demand by the civil rights organisation Justice that the exemption for "participant monitoring" under IOCA should be addressed.[33]

Clause 4 lists the cases where a power may be taken to provide for lawful interception without the need for a warrant under Clause 5. These include:

- A communication service provider located in the UK which is providing a public telecommunications service to another country may be authorised to use

---

29 Ibid, para 25

30 Ibid, para 31

31 In this instance, the interception would constitute "directed surveillance" as defined in Clause 25(2) and Clause 45(4)

32 Bill 64 – EN, para 36

33 Justice's response to the government consultation paper '*Interception of Communications in the United Kingdom*', para 1.15, in Dep 99/1773, also available at http://www.homeoffice.gov.uk/oicd/iocresp.htm

telecommunications systems located in the United Kingdom to intercept the communications of subjects on the territory of another country in accordance with the law of that country, in accordance with Article 17 of the draft Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union[34]

- The Secretary of State may make regulations permitting certain kinds of interception in the course of business transactions (for example, monitoring the public's transactions with call-centres in order to provide evidence of those transactions)[35]
- Prisoners' communications may be monitored in accordance with the *Prison Rules*
- The communications of high security patients who are detained under the *Mental Health Act 1983* may be monitored in accordance with directions under section 17 of the *NHS Act 1977*.

The second reading briefing on the Bill by the civil liberties organisation Liberty comments that the provisions relating to prisons and secure hospitals in Clause 4 are "unacceptably open-ended".[36]

2. Warrants

Clause 5 allows the Secretary of State to issue a warrant authorising or requiring interception to be carried out. *Subsection (2)(b)* introduces a proportionality test: under human rights case law, any interference with a Convention right must be proportional to the intended objective. The civil liberty organisation Liberty, while welcoming this provision, suggests that it will be weakened in practice by problems with *subsections (3) and (4)* (see below).

Subsection (3) sets out the grounds on which the Secretary of State may issue warrants:

(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.

The Explanatory Notes comment that the Secretary of State may not issue a warrant

> unless he considers that the warrant is necessary on one of those grounds. It would not therefore be sufficient for him to consider that a warrant might be useful in supplementing other material, or that the information that it could produce could be interesting. The word 'necessary' reflects the wording of Article 8 of the Convention – "necessary in a democratic society".[37]

---

34 Compare Clause 1(4)
35 See also Clause 1(6)
36 28 February 2000
37 Bill 64 – EN, para 52

Liberty suggests that the grounds set out in subsection (3) "suffer from the same defects as the corresponding provision of IOCA":

> "National security" and "economic well-being" are extremely vague and subjective ideas. The Bill defines neither. If activity is so great a menace to society as to justify interference with fundamental rights of the citizen, one would expect it to be prohibited by the criminal law, with the definitional certainty that attracts. Subject only to well-defined exceptions, "prevention or detection of serious crime" should be the sole ground for authorising interception.
>
> In the field of national security, a range of crimes of espoinage, terrorism and conspiracy cover an enormous range of harmful conduct. In the filed of economic well being. Offences covering fraud, evasion of fiscal nad customs regulation, insider dealing, false accounting, counterfeiting and so forth prohibit an equally broad range of objectionable activity. If Parliament has not judged an activity sufficiently grave or insidious to justify bringing it within the criminal law, then it should not generally be regarded as a legitimate basis for interception or surveillance.
>
> The definition of "serious crime" (clause 71(4)) should not include the "common purpose" head. That unjustifiably extends the net of surveillance indiscriminately to participants in legitimate collective activity - industrial action, organised protest and so on - who are not themselves suspected of inherently serious wrongdoing. That cannot be regarded as proportionate. It is also likely to deter individuals from exercising the right of freedom of association protected by the Human Rights Act.[38]

Under *subsection (4)*, the matters to be taken into account in considering whether the interception is necessary or proportionate must include

> whether the information which it is thought necessary to obtain under the warrant could reasonably be obtained by other means.

Liberty states:

> Clause 5(4) effectively replicates the unsatisfactory IOCA requirement that the Secretary of State merely "consider" the availability of alternative means of obtaining the relevant information. Where access is sought in cases of routine crime to confidential or other sensitive material, Schedule 1 to the Police and Criminal Evidence Act 1984 requires the investigating authority to positively show that other methods have failed or are bound to fail. For the Bill to apply a less stringent test where the individual faces an interference with fundamental rights on the basis of suspicion of serious wrongdoing turns proportionality on its head.[39]

---

[38] Regulation of Investigatory Powers Bill, Second reading briefing, Liberty, 28 February 2000

[39] Ibid

Clauses 6 and 7 deal with who may apply for and who may sign interception warrants. In all but urgent cases, the warrant must be signed by the Secretary of State. The Explanatory Notes observe that even in urgent cases - where warrants may be signed by a senior official - the Secretary of State must have given personal consideration to the application, in order to give instructions to that official for the signing of that particular warrant, which will be limited in duration to five working days.[40] However, **Clause 10**, in contrast to the equivalent provision in IOCA, enables a senior official to modify warrants which the Secretary of State has already signed.

Under **Clause 8** warrants must specify the person or the set of premises to be intercepted. This introduces a change to the corresponding provision in IOCA: under Clause 8 it will be possible to use a single warrant authorising interception of all specified communications addresses relating to the named person.

Clause 9 deals with the duration, cancellation and renewal of warrants. The duration of various categories of interception warrant is extended in comparison with the equivalent provision in IOCA. **Clauses 14 and 15** deal with general safeguards on the implementation of warrants and extra safeguards in the case of certified warrants (ie those to which Clause 8(3) applies).

One of the most controversial aspects of the existing legislation has been the procedure for issuing warrants authorising the interception of communications. Chapter 7 of the consultation paper stated:

> The law currently requires interception to be personally authorised by the Secretary of State. This is done by the facts of the case being presented to the Secretary of State who considers whether the use of interception is justified. If he or she decides that it is, they sign the warrant which authorises interception to be carried out. The warrant is then served upon the PTO or Post Office. In an emergency, it is possible for a warrant to be issued by a senior civil servant, but only after the Secretary of State has been briefed on the case and has given his or her specific authority.
>
> Other authorisation frameworks have been examined during the review of IOCA, including judicial warranting or a system based upon the model of the Police Act 1997. While both would have advantages, particularly in their ability to meet the operational needs of the Agencies, there would remain the need for the Executive to issue warrants applied for on national security or economic well-being grounds, perhaps leading to parallel warranting arrangements.
>
> The alternative options have been carefully considered and compared with the existing Secretary of State warranting procedures. On balance, the Government is not persuaded of the need to depart from the current means of authorising interception of

[40] Bill 64 – EN, para 65. "Senior official" is defined in Clause 71(1)

> communications and proposes to continue with the long established principle of Secretary of State authorisation.

The Government's analysis of the responses to the consultation paper noted that "around ten" responses argued that warrants should be authorised by members of the judiciary rather than the Secretary of State, particularly in serious crime cases.[41]

The response to the consultation paper by the civil rights organisation Justice stated:

> JUSTICE's preferred position is set out in our 1998 report: authorisations for telecommunications interceptions should be given by a person holding high judicial office. This is the practice in a great number of other countries, including Canada, New Zealand, the United States, and European Union Member States. It would also have the additional advantage of bringing the law on the interception of telecommunications in line with the Police Act regime for intrusive surveillance. There are also practical considerations for favouring a judicial authorisation regime: the sharp rise in the number of serious crime applications makes it increasingly impractical for the Home Secretary to scrutinise all applications in person. Judicial authorisation may also assist in some of the evidential problems referred to in paragraphs 4. 1 -11 below.
>
> JUSTICE does not consider that the single reason provided in the Consultation Paper against judicial authorisation-the need for a separate regime for police and the security and intelligence services-is compelling. Not only is this common practice in other countries, such as Australia; but also a parallel regime for intrusive surveillance by police and the security services already exists in the UK under Part Ill of the Police Act 1997 and the Intelligence Services Act 1994.[42]

The Data Protection Commissioner[43] and the civil liberties organisation Liberty also support a system of judicial authorisation for interception of communications. Liberty's second reading brief on the *Regulation of Investigatory Powers Bill* stated:

> Retention of executive rather than prior judicial authorisation of interception is fundamentally objectionable. That the executive should secretly authorise itself to commit clandestine interferences with important rights is neither acceptable nor necessary.
>
> The Government has failed to advance any satisfactory case for failure to adopt a judicial procedure. Prior judicial sanction operates well in routine criminal investigations (PACE 1984 Schedule 1: application to a circuit judge) and forms a satisfactory basis for clandestine interception arrangements in other European countries, including Germany.

---

41 Dep 99/1666, December 1999, also available at: http://www.homeoffice.gov.uk/oicd/iocresp.htm
42 Dep 99/1773, available on the internet at: http://www.homeoffice.gov.uk/oicd/iocresp.htm
43 Formerly the Data Protection Registrar

> Judicial involvement maintains public confidence in the investigatory framework. It would eliminate the risk of a débacle such as the Matrix Churchill affair.
>
> We consider it essential that in all cases covered by clause 5, authority to intercept should be sought from a High Court or equivalent judge.[44]

The Data Protection Commissioner's response to the Bill stated:

> The Act of intercepting any communication justifies strict controls. While problems might arise in this area in relation to warrants obtained for the purposes of safeguarding national security, the same complications do not arise in relation to the interception of communications for the purpose of preventing or detecting serious crime.
>
> If information were obtained under a judicial warrant where the interception was related to the prevention and detection of crime the intercept product would be admissible in evidence in legal proceedings. This would also allow for judicial scrutiny of the procedure at a later date and would provide an alternative to the Tribunal as a forum for dispute resolution.
>
> Two separate systems could be established, whereby judicial warrants would be more appropriate for use in relation to criminal matters and administrative warrants would mainly be relied upon in cases involving national security.[45]

3. New Duties for Communications Service Providers

Under **Clause 11**, where communications service providers (CSPs) are required to give assistance to the police etc in accordance with an interception warrant, they must do everything reasonable required of them in order to effect the interception. **Clause 12** enables the Secretary of State to oblige CSPs to maintain a reasonable intercept capability. Under **Clause 13**, the Secretary of State is permitted but not required to make contributions towards costs incurred by communications service providers in providing an intercept capability.[46]

The Government's analysis of the responses to the consultation paper stated:

> This aspect of the consultation paper produced the most response, mostly from CSP interests; and a number of points were made about the nature of any requirement. There was a general acceptance of the basic principle that legally binding requirements could be imposed on CSPs to intercept traffic on their network, but less agreement about how costs should be allocated. The following points were made. It

---

[44] 28 February 2000

[45] *Response of the Data Protection Commissioner to the Government's Regulation of Investigatory Powers Bill*, a briefing for Parliamentarians, March 2000, paras 4-7

[46] Compare Clause 23 which requires the the Secretary of State to make appropriate payment arrangements to compensate holders of communications data for the costs involved in complying with their duty to supply such data.

> would be necessary to have a great deal of consultation between Government and industry, in order to develop a clear expression of what was actually required. A definition must be functional, not based on any particular technologies as these were in rapid flux. The requirement must not be too restrictive on business, or impose a greater burden than in the rest of Europe. It must be transparent to the entire business community and enforced uniformly. And law enforcement and security and intelligence agencies would need to develop considerable expertise themselves to handle the intercepted material; CSPs should not be expected to do all the processing required.
>
> The proposal to arrange for independent and impartial advice to the Secretary of State on what constitutes a reasonable requirement was welcomed. Some business interests were uncomfortable with the idea of OFTEL providing this advice, and felt representatives from industry should also be included. The ACPO/ISP forum was suggested for this role.[47]

The Data Protection Commissioner stressed that the Government should not place obligations on CSPs which require them to take steps which might jeopardise the privacy rights of their customers. A requirement to maintain an intercept capability

> must be balanced against the need to maintain appropriate security, and service providers should guard against adopting lesser standards which could facilitate unauthorised access to communications as well as authorised access. This would have serious implications for the privacy rights of individuals and could have consequences for consumer confidence in relation to on line communications which in turn might jeopardise the growth of e-commerce.[48]

4. Use of Intercept Evidence in Court

With certain exceptions, **Clause 16** excludes evidence, questioning or assertion in legal proceedings likely to reveal the existence or absence of a warrant. In other words, intercept material cannot be used as evidence in court. This mirrors a similar provision in section 9 of the *Interception of Communications Act 1985*, which this Bill repeals. The exceptions are laid down in **Clause 17**, which goes beyond the exceptions contained in s9 of the 1985 Act. Thus intercept material may be used in evidence:

- in any proceedings before the Special Immigration Appeals Commission;
- in any legal proceedings relating to the fairness or unfairness of a dismissal on the grounds of any conduct constituting an offence under Clause 1(1) or (2), 11(7) or 18 or Section 1 of *Interception of Communications Act 1985*;

---

47 Dep 99/1666, December 1999, also available at: http://www.homeoffice.gov.uk/oicd/iocresp.htm

48 Dep 99/1773, available on the internet at: http://www.homeoffice.gov.uk/oicd/iocresp.htm. See also Trade and Industry Select Committee, *Building confidence in Electronic Commerce: The Government's proposals*, HC 187 of 1998-99, May 1999, Minutes of evidence

- if the interception is lawful without the need for a warrant by virtue of Clauses 1(5)(c), 3 or 4 (for example, where all parties to the communication consent to the interception; one of the parties to the communication consents to its interception *and* it is authorised by a police officer etc. on one of the grounds contained in Clause 27(3); or a circuit judge orders that stored data relating to messages previously sent to a pager be produced under Schedule 1 to the *Police and Criminal Evidence Act 1984*).

In addition, Clause 17(5)(a) provides that the fact and contents of an interception may be disclosed to a person conducting a criminal prosecution, who has a duty, recognised in case law, to ensure that a prosecution is fair.

The question of whether intercept material should be used as evidence in criminal prosecutions has been the subject of long debate. Lord Lloyd's *Inquiry into Legislation Against Terrorism* observed that

> One of the themes which has persisted throughout the Inquiry is the difficulty of obtaining evidence on which to charge and convict terrorists, particularly those who plan and direct terrorist activities without taking part in their actual execution. This has proved to be a serious weakness in the anti-terrorist effort, especially in Northern Ireland. In many cases the leaders of the paramilitary organisations may be known well enough to the police, but there is insufficient evidence to convict them.[49]

Lord Lloyd observed that under section 9 of the *Interception of Communications Act 1985*, the product of telephone interceptions was inadmissible as evidence "however compelling the evidence might be to prove the defendant's guilt". The effect of s9 had been reinforced by various provisions in the *Criminal Procedure and Investigation Act 1996*. He argued that the strict embargo on intercept evidence should be relaxed in terrorist cases. His arguments were as follows.

First, importance evidence may be unavailable to the prosecution authorities as a result of the embargo:

> The United Kingdom stands alone in excluding such material. Thus in the United Stages the use of intercept material in evidence is regarded as essential. In many instances, including high-profile cases involving the New York Mafia, convictions otherwise unobtainable have been secured by the use of intercept material. […]
>
> I have been shown a list of some twenty cases, including four recent cases in which the intercept material would have been of assistance to the prosecution; and I was told of at least one terrorist investigation in which the interception evidence would have

[49] Cm 3420, October 1996, Vol 1, p33

> supplied "the missing pieces in the jigsaw" and thus enabled a prosecution to be brought.[50]

Second, there is a "curious disparity" between telephone tap material obtained under the 1985 Act, which may not be used in evidence, and material obtained as a result of other kinds of surveillance, which may. This distinction is maintained in the current Bill: there is no equivalent of Clause 16 in the parts relating to other kinds of investigatory powers. Lord Lloyd identified a further "anomaly":

> In drugs cases, and other cases involving an elleged conspiracy, the prosecution often rely on the frequency of telephone conversations between two or more subscribers to prove the conspiracy. *R V Preston* was just such a case.[51] The police can obtain this information without difficulty from the telephone operating company, since the company needs the information for the purpose of billing its customers. Hence the term "metering". There is nothing in IOCA [the 1985 Act] to prevent the prosecution from adducing metering evidence, and inviting the jury to infer from the pattern and frequency of telephone calls that the defendants are parties to a conspiracy. It would surely seem odd to a member of the jury that he was being invited to infer guilt from the happening of one or more telephone conversations without being told what was actually said. Is it sensible that the prosecution should be obliged to get round the prohibition contained in section 9 of the Act by this indirect means?[52]

The current Bill changes this feature of the law. Chapter II contains separate provision regulating the acquisition of metering information ("communications data"). Clause 16 would prevent the use of metering evidence in cases where a warrant to intercept telephone calls had been obtained under Chapter I, but not in other cases.

Lord Lloyd presented the arguments in favour of the embargo on intercept material as evidence as follows. First, it has been claimed that

> if interception material is used as evidence in court, the intercept capability will become more widely known among terrorists, drug dealers and the criminal classes generally; as a result criminals would use more guarded language, or avoid the use of the telephone altogether.[53]

Lord Lloyd argued that

> There is no evidence that the intelligence effort in other countries – eg the United States or Australia – has been affected in any way by the use of intercept material in court. […] Sophisticated criminals are all well aware that their telephones are, or

---

50 Ibid, p35
51 *R v Preston* (1994) AC 130 at page 163
52 Cm 3420, Op cit, Vol 1, p36
53 Ibid

> may be, tapped. This is why they adopt coded language when discussing their plans, and often use telephones which they think may not be tapped.[54]

The second argument against the relaxation of the embargo is that it will result in pressure for increased disclosure by the prosecution. Lord Lloyd commented:

> This would certainly be the consequence in any case in which the prosecution choose to rely on intercept evidence. Obviously in such a case the defence would be entitled to see the whole of the interceopt evidence relating to that defendant. But where the prosecution chooses not to rely on intercept evidence, the position will be the same as it is today. The prosecution will not be obliged to disclose the existence of any intercept material, and the defence will not be permitted to ask whether such material exists.[55]

Lord Lloyd also raised the fear that the use of intercept material will add to the burden of the prosecution in preparing for trial, and to the expense of the agencies in storing intercept material pending a decision by prosecuting counsel on whether he intends to use the material or not. He emphasised that he only proposed that the embargo on intercept evidence should be lifted in terrorist cases. He doubted that the use of intercept material would add to the burden on prosecution counsel, since the prosecution must in any event be satisfied that there is nothing in the material which is inconsistent with the defendant's guilt.

The consultation paper *Interception of Communications in the United Kingdom*[56] sought suggestions for a regime which would enable intercept material to be used in evidence and to make appropriate disclosures to the defence, bearing in mind the effects upon sensitive information, resources and the efficient operation of the criminal justice system. The paper noted that in addressing this issue, the Government would have to bear in mind the requirement of Article 6 of the European Convention on Human Rights, which guarantees the right to a fair trial:

> Implicit in this guarantee is the principle that there must be "equality of arms" between the prosecution and the defence in criminal proceedings. Any rule of evidence or procedure which favours one party over the other may conflict with this principle.
>
> The question of whether section 9 of IOCA undermines the principle of "equality of arms" and introduces an unfairness into proceedings where interception played a part in the investigation was addressed by the European Commission in the case of *Preston v UK*. The applicants claimed, amongst other things, that their trial was unfair because knowledge of material gathered through interception of communications gave the prosecution an advantage in preparing their case. They also claimed that the use in evidence of data relating to communications, while interception material was

---

54 Ibid, p37
55 Ibid
56 Cm 4368, June 1999, chapter 8

> excluded, amounted to an inequality of arms. The Commission did not agree, noting that section 9 prevented either party adducing evidence which could tend to suggest that interception had taken place. The Commission did not consider that the applicants had shown how access to interception material by the police had any effect on subsequent proceedings, or in what respect that material was used to the applicants' detriment in preparing the prosecution case, other than to provide the prosecuting authorities with a starting point from which to gather admissible evidence against the applicants. The Commission, by a majority, declared the application inadmissible.
>
> In many other European states, intercept evidence is used in criminal cases and, so far as Article 6 is concerned, this practice has been approved by the European Court. See, for example, *Valenzuela Contreras v Spain* (30 July 1998) and *Lambert v France* (24 August 1998).
>
> However, in those States interception is generally ordered by an investigating judge. The United Kingdom is in a different position, since criminal investigations are not supervised by judges but by the law enforcement agency. For that reason, the principle of equality of arms as between prosecution and defence will be particularly relevant in devising any system which allows the use of intercept material in evidence. Furthermore, any arrangements which made intercept material available to one or both parties would have to be both practical and affordable.
>
> To date, no satisfactory arrangements have been found. Nevertheless, the Government continues to work on the question, and would welcome the views of others.

In its analysis of the responses to the consultation paper, the Government noted that just over half of the 85 respondents commented on this issue:

> Roughly two thirds of these respondents (the majority of communications service providers [CSPs] and police forces) wished the prohibition to remain, CSPs on the grounds of staff safety and staff time spent in court. Those in favour of its abolition were mostly civil liberty organisations, and some police forces.[57]

The Criminal Bar Association's response supported the use of intercept evidence as evidence. The arguments it deployed mirrored those set out in Lord Lloyd's report. It also suggested that:

> As a matter of principle, if intercept material implicates an accused the prosecution should be able to benefit from it. Conversely, if it reveals conversations tending to assist the defence then it should be capable of adduction in the accused's favour[58]

The Criminal Bar Association Issues also raised issues concerning international co-operation:

---

[57] Dep 99/1666, December 1999, also available at: http://www.homeoffice.gov.uk/oicd/iocresp.htm

[58] Dep 99/1773, available on the internet at: http://www.homeoffice.gov.uk/oicd/iocresp.htm

> In the context of crime with an international dimension, foreign agencies regularly supply our own law-enforcement agencies with their own intercept material. Where such material has been gathered according to the law of the foreign state, it is admissible in the UK: Aujla and others (1998) 2 Cr. App. R 16.
>
> In those circumstances, policy considerations applied by UK prosecuting authorities (eg HM Customs and Excise) have prevented the use of such material in evidence here. The result is the worst of both worlds in that the material is (with the knowledge and consent of the foreign donor agency) disclosed to the defence in full but not used in evidence. Capability is revealed without use being made of the probative material.

However, the Lincolnshire Constabulary suggested that:

> The biggest problem with the use of intercept material in evidence is one of practicalities and cost due to disclosure rules. There is no doubt a defence lawyer would require the transcript of the conversations and in most operations of this scale it would take months and in some cases years to type the transcript. The cost of this would be immense.[59]

The Data Protection Commissioner's briefing on the current Bill links the issue of the admissibility of intercept evidence to the question of whether judicial authority for warrants should be required (see above).

Comments on the consultation paper by William George Carmichael, a member of the Interception of Communications Tribunal, strongly supported the use of intercept evidence, but noted that

> The problem of course is that if such evidence is given the door is opened for the Defence in cross examination to explore the workings of the Agency and the inner secrets of interception would be disclosed to the public domain.[60]

Mr Carmichael's response contains suggestions on how to overcome this problem and the consequential implications for the requirement under Article 6 of the European Convention on Human Rights that there must be equality of arms between the prosecution and the defence.

5. Communications Data

Chapter II of the Bill provides a legislative framework for the police and security services etc to obtain communications data (ie. information relating to the use of a communications service but not the contents of the communication itself). It is intended to create a system of safeguards, reflecting the requirements of Article 8 of the European Convention on Human

---

59 Ibid
60 Ibid

Rights (the right to respect for private and family life). **Clause 21** identifies the situations in which communications data may be obtained. These are somewhat wider than the grounds on which communications themselves may be intercepted:[61]

> (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;
>
> (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.

Liberty's second reading brief on the Bill states:

> Clause 21 permits access to such data on broader grounds than apply to interception proper. The underlying assumption that data access represents a lesser intrusion into rights of privacy than interception is misconceived. The grounds should be no wider than we recommend in relation to interception.[62]

Clause 21 incorporates twin tests of necessity and proportionality which mirror those in relation to the interception of communications under Clause 5. **Clause 23** requires the Secretary of State to make appropriate payment arrangements to compensate holders of communications data for the costs involved in complying with their duty to supply such data.

The Government's analysis of the responses to the June 1999 consultation paper (Cm 4368) stated:

> There was an almost equally balanced split between those who welcomed the inclusion of this aspect of communications in the IOCA regime and those who felt that it should be left separate and in the Data Protection Act regime. Various suggestions were made as to who should authorise requests: internal to agency; at

---

61 See Clause 5(1)

62 28 February 2000

> Secretary of State level; or by a judge. Some CSPs felt that requests for communications data should be more tightly controlled.[63]

The Data Protection Commissioner welcomed the Government's decision to create a framework for access to communications data, since section 29 of the *Data Protection Act 1998*, under which such data is currently disclosed to investigatory bodies, "does not provide a satisfactory basis for large scale disclosure".[64] She stated, however, that

> It is essential that the new arrangements do not simply provide a statutory basis for investigating bodies to obtain easy access to communications data where this is not justified. […] The grounds for wishing to obtain certain communications data should be subject to prior external scrutiny, ideally by a judge. At the very least the procedures for authorising such access should be subject to scrutiny by an independent person or body in order to provide the necessary public reassurance that the proper procedures are being followed.

Chapter II does not require judicial authorisation for the acquisition by the police etc of communications data, but the remit of the new Interception Commissioner appointed under Clause 53 will include the operation of the communications data regime.

B. Part II: Surveillance and Covert Human Intelligence Sources

The Government's stated aim for this part of the Bill was set out as follows:[65]

> Intrusive investigative techniques often provide vital intelligence in solving serious criminal activity and terrorism, but such criminals can be well-versed in anti-surveillance measures. To combat this type of criminal the police, HM Customs and the security and intelligence services must be able to use the most effective technology available. It is essential that we safeguard these techniques - while at the same time ensuring that they are properly controlled and those employing them are accountable. It is important, too, that other public authorities who use these techniques also comply with properly regulated controls and procedures.
>
> - The Bill proposes to put the use of covert surveillance not already covered by Part III of the Police Act 1997 and the Intelligence Services Act 1994, and the use of covert human sources - that is, informants, agents and undercover officers - on a statutory footing.

The legislation would cover the use of intrusive investigative techniques by the police, the National Criminal Intelligence Service, the National Crime Squad, HM Customs and Excise,

---

63 Dep 99/1666, also available on the internet at: http://www.homeoffice.gov.uk/oicd/iocresp.htm

64 *Response of the Data Protection Registrar to the Government's Proposals for Revising the Interception of Communications Act 1985*, Dep 99/1773, also available on the internet at: http://www.homeoffice.gov.uk/oicd/iocresp.htm

65 *Regulation of Investigatory Powers Bill Published Today*: Home Office Press Release 022/2000 10 February 2000

MI5, MI6, GCHQ, Government Departments and other public authorities who carry out an enforcement or investigative role. **Clause 26** provides that authorisations may be granted under this part of the Bill for surveillance outside the United Kingdom.

Clause 25 defines three types of activity which are covered by part II:

- **Directed surveillance** is covert surveillance that is undertaken in relation to a specific investigation in order to obtain information about, or identify, a particular person or to determine who is involved in a matter under investigation. Directed surveillance may also include the interception of communications where there is no interception warrant and where the communication is sent by or is intended for a person who has consented to the interception.[66]

- **Intrusive surveillance** is covert surveillance carried out in relation to anything taking place on residential premises or in any private vehicle. This kind of surveillance may take place by means either of a person or device located inside residential premises or a private vehicle or by means of a device placed outside which consistently provides a product of equivalent quality and detail as a product which would be obtained from a device located inside. Under *subsection (4)*, the use of tracking device is not intrusive surveillance.

- A person is a **covert human intelligence source** if he or she -
  (a) establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);
  (b) covertly uses such a relationship to obtain information or to provide access to any information to another person; or
  (c) covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

Clause 44 enables the Secretary of State, by order under the affirmative procedure, to change the types of activities which fall within the categories of intrusive and directed surveillance by providing that a type of directed surveillance will be treated as intrusive surveillance or vice versa.

The Data Protection Commissioner has made the following comments on these definitions:

1. The definition of intrusive surveillance should be widened to include "any premises or location where the individual has a legitimate expectation of privacy, for example, a doctor's surgery or an MP's private office."[67]

---

66 Clause 45(4). See also Clause 3

67 *Response of the Data Protection Commissioner to the Government's Regulation of Investigatory Powers Bill*, a briefing for Parliamentarians, March 2000, para 10

2. Intrusive surveillance as currently defined excludes surveillance which takes place by means of external devices which do not provide a product of equivalent quality and detail as internal devices:

> It is the view of the Commissioner that external surveillance devices, for example long lens photographic equipment, can be used in an intrusive manner, providing sufficient detail to infringe the privacy of the individual, even when the information obtained is not of the same quality or detail as may be obtained by a device located on the premises or in the vehicle. The fact that a picture from a long lens camera might not be quite as clear as from a camera placed in the room does not necessarily make the infringement of privacy any less.[68]

3. The Bill defines surveillance as 'covert' under Clause 25(8)(a) "if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place".

> It is the view of the Commissioner that the surveillance should be regarded as covert if the effect is that persons are unaware that it is being carried out. It should not be defined on the basis of whether it is the intention of those carrying out the surveillance to ensure that the persons are unaware. It is whether the person is in fact aware that is important. This is the approach taken in the Data Protection Act 1998 which requires the provision of prior information to data subjects to make processing of their personal data fair.[69]

Liberty's second reading brief makes the following points about part II of the Bill:

> The gathering and use of information about the citizen through each of the three techniques to which this Part applies (clause 25(1)) interfere with rights under Article 8 of the Convention. The proposed scope of the powers and procedural safeguards in relation to authorisation raise issues similar to those arising under Part I.
>
> This Part applies to a wider variety of investigative objects including detection and prevention of routine rather than just serious crime. We accept that greater flexibility is appropriate as regards the grounds on which activity may be authorised and the content of the authorisation procedure.
>
> However, the requirement of proportionality means that the more that is at stake for the suspect - that is, the more intrusive the technique in question and the more serious the allegation against the target - the greater the necessary safeguards.
>
> Clauses 28 and 29 are therefore unsatisfactory because proposing a single, wide set of grounds, and a system of wholly executive authorisation, to all the possible kinds of operation covered by the Part. The proposal for "second-guessing" certain authorisations by a Surveillance Commissioner (clauses 33-35) does not adequately

---

[68] Ibid, para 11
[69] Ibid, para 12

> address the problem. We will support amendments aimed at ensuring that operations involving serious interferences with rights are authorised on appropriately defined grounds and by prior judicial sanction.[70]

Clauses 41 to 43 set out general rules for the grant, renewal and duration of surveillance authorisations under part II of the Bill. **Clause 45** defines some of the terms used in this part of the Bill.

1. Directed Surveillance and Use of Undercover Officers

Clauses 27(3) & 28(3) list the grounds on which these forms of surveillance may be authorised. These are the same as those in Clause 21, except that the grounds cited there of preventing death or injury in an emergency is not repeated, and are wider than the grounds for intercepting communications listed in Clause 5(3). Thus, for example, directed surveillance or undercover officers may be used for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department, or for other purposes which may be specified by order of the Secretary of State. As noted above, the civil liberties organisation Liberty believes that these grounds are too wide.

As with other forms of surveillance covered by the Bill, it must be both 'necessary' and 'proportionate'.[71] The Secretary of State may make orders to prescribe who within relevant public authorities may authorise directed surveillance and covert human intelligence sources **(Clause 29)**. It is anticipated that this will be specified in the draft Code of Practice which is likely to be issued soon. The Data Protection Commissioner has commented:

> Authorisation of intrusive surveillance for law enforcement purposes should be based on a judicial warrant because the invasion of privacy is comparable to the cases of the interception of communications and third party access to encrypted information. Further, criminal sanctions should be applied where appropriate authorisation has not been sought. There is no provision for any criminal sanction in the Bill in relation to unauthorised intrusive surveillance.[72]

2. Intrusive surveillance

Under **Clause 30**, intrusive surveillance must be authorised by:

(a) a chief constable or chief officer in the case of the police, NCIS, NCS and Customs & Excise, or
(b) the Secretary of State in the case of the security services, government departments, etc.

---

[70] 28 February 2000

[71] See, for example, Clause 5, covered in part II(A)2 of this paper

[72] *Response of the Data Protection Commissioner to the Government's Regulation of Investigatory Powers Bill*, a briefing for Parliamentarians, March 2000, para 13

Here too, the surveillance must be both 'necessary' and 'proportionate'. The grounds for authorisation are narrower than those for directed surveillance and covert human intelligence sources: they are defined in terms of national security, preventing or detecting serious crime or the economic wellbeing of the United Kingdom.[73]

Clauses 32 to 37 set out the procedure for obtaining intrusive surveillance authorisations for investigations carried by the police, NCIS, NCS and Customs & Excise. They outline very similar procedures to those set out in part III of the *Police Act 1997*:

- the initial authorisation of an intrusive surveillance operation must be given by the chief constable, etc, except where this is not practicable in urgent cases
- approval from a Surveillance Commissioner[74] will be required before an authorisation can take effect, except in urgent cases
- in urgent cases authorisations may take effect without prior approval of a Commissioner, but the chief constable etc will have to notify a Commissioner as soon as reasonably practicable, giving reasons for proceeding without approval.
- a Commissioner will approve an operation only if he is satisfied that the action meets the dual test of necessity and proportionality
- under Clause 35 a Surveillance Commissioner may quash an authorisation if he or she believes that the criteria for authorisation in Clause 30 were not met at the time the authorisation was granted or renewed, or that there are *no longer* any reasonable grounds for believing that the criteria in Clause 30 are met.
- a chief constable etc may appeal to the Chief Surveillance Commissioner against a refusal of a Surveillance Commissioner to approve an authorisation or renewal, etc

Clauses 39 and 40 deal with those intrusive surveillance authorisations granted by the Secretary of State. The relevant agencies are:

(a) the intelligence services;
(b) the Ministry of Defence;
(c) Her Majesty's forces;
(d) an individual holding an office, rank or position with any such public authority as may be designated for the purposes of this section as an authority whose activities may require the carrying out of intrusive surveillance.

In general, the grounds on which intrusive surveillance may be authorised for these agencies are as set out in Clause 30, although **Clause 39(3)** limits the grounds on which MOD or the

---

[73] Thus they mirror the grounds contained in Clause 5(3) except for the additional ground relating to international mutual assistance. See part II(A)2 of this paper

[74] A Commissioner appointed under part III of the *Police Act 1997*

Armed Forces may be granted a warrant to investigations carried out in the interests of national security or the prevention or detection of serious crime (not, in other words, for the economic well-being of the United Kingdom). **Clause 40(3)** prevents MI6 or GCHQ from being granted a warrant for intrusive surveillance in the British Islands for investigations carried out for the prevention or detection of serious crime.

C. Part IV: Scrutiny of Investigatory Powers and Codes of Practice

1. Commissioners

Clause 53 creates a new Commissioner, the Covert Investigations Commissioner, and replaces the existing Commissioner appointed under the *Interception of Communications Act 1985* with an Interception of Communications Commissioner. Both posts would be appointed by the Prime Minister. **Clause 54** creates a duty to cooperate with the Interception Commissioner and Covert Investigations Commissioner and to provide documents and information. **Clause 55** adds to the existing roles of the Security Service Commissioner, Intelligence Services Commissioner and Surveillance Commissioner oversight of various activities covered by the current Bill. This means that:

1.The Interception Commissioner will oversee the use of interception of communications powers.

2. The use of other surveillance methods authorised by the Bill will be overseen by:

- The Security Service Commissioner, in the case of MI5
- The Intelligence Services Commissioner, in the case of MI6, GCHQ and MOD
- The Surveillance Commissioner, in the case of the police etc and Customs & Excise
- The Covert Investigations Commissioner, in the case of other authorities given powers under the Bill.

2. The Tribunal

Clause 56 establishes a Tribunal, with the members to be appointed by Her Majesty by Letters Patent. It will consider various matters including complaints against the intelligence services and complaints relating to the powers covered by the Bill. It is designed to be the appropriate forum for the redress of Convention rights in respect of these matters. The Tribunal's jurisdiction, procedure and rules are set out in **clauses 57 – 60**. The Tribunal will replace the existing functions of tribunals established under the *Security Service Act 1989*, the *Interception of Communications Act 1985*, the *Intelligence Services Act 1994* and the *Police Act 1997*.

The Government's analysis of the responses to the June 1999 consultation paper observed:

> A couple of industry bodies said that communications service providers should be able to contact the Commissioner/Tribunal directly; one reason for this would be to

ensure that their business was protected from civil liabilities from interception by the State. A few groups suggested that those who have been intercepted should be notified of the fact at a later date - an idea that law enforcement felt to be unworkable – and maintained that a more open tribunal system would be required to comply with the European Convention on Human Rights. The fact that the Tribunal does not assess the factual basis of a decision was criticised. The fact that the Tribunal had never upheld a complaint was a matter of concern for many respondents.[75]

Liberty's second reading brief on the Bill states:

The Tribunal proposed by the Bill is potentially a considerable improvement on the present restrained and secretive separate tribunal systems. However, it also preserves number of serious deficiencies in the present framework.

Disposal of complaints

The Tribunal should have power to review the substantive merits of authorisation of the interception, surveillance or other measures in question. It should not be confined to the narrow grounds on which an application may be made for judicial review (clause 58(2) and (3)). That restriction will lead in many cases to violation of Article 6 of the Convention.

The Tribunal's determination should give an adequate indication of its findings on the issues raised by the complaint. The cryptic determination proposed by clause 59(4) falls short of even the most modest requirements of fairness in judicial decision-making.

There should be an express statutory right of appeal from the Tribunal to the High Court on a point of law. The draft Electronic Communications Bill 1999 proposed this in relation to what is now Part III of the Bill. That proposal has now been commuted to the wholly unsatisfactory clause 58(8).

Procedure

Clause 60 raises the prospect of a significant step forward from the present statutory framework, whose various tribunals fall well short of the requirements of fairness and transparency required in a modern democracy, even allowing for the particular demands of their subject-matter. The test to be applied by the Secretary of State when making procedural rules (clause 60(6)), and by the Tribunal itself when applying them, should be one based firmly on proportionality: any derogation from the usual standards of fairness and publicity associated with court and tribunal proceedings should be permitted only to the strict extent necessary in pursuance of the demonstrable requirements of national security or operational secrecy.[76]

---

[75] Dep 99/1666, also available on the internet at: http://www.homeoffice.gov.uk/oicd/iocresp.htm

[76] 28 February 2000

3. Codes of Practice

The Secretary of State will be required to issue Codes of Practice relating to the exercise and performance of the powers and duties contained in this Bill and also and those relating to interference with property or wireless telegraphy in either the *Intelligence Services Act 1994* or part III of the *Police Act 1997* **(clause 62).** Such codes will be subject to consultation and drafts must be laid before Parliament and brought into force through an Order by affirmative resolution.

D. Part V: Miscellaneous and Supplemental

Clauses 64 - 66 amend the *Wireless Telegraphy Act 1949*, the *Intelligence Services Act 1994* and the *Police Act 1997* to introduce, amongst other things, the tests of necessity and proportionality seen elsewhere in the Bill (for example at Clauses 5 and 21) which are deemed necessary in order to comply fully with the *Human Rights Act 1998.*

Clause 69 provides that a director, etc of a body corporate may in certain circumstances be held personally and criminally liable for an offence under the Bill which is committed by that body corporate, for example the unlawful interception of communications.

III Part III of the Bill: Encryption

Part III of the *Regulation of Investigatory Powers Bill* is an amended version of Part III of the Draft *Electronic Communications Bill*, published in July 1999.[77] Although the Draft Bill formed the basis of the *Electronic Communications Bill* (Bill 33 of 1999/2000), Part III was omitted because of concern as to whether it would be compatible with the *Human Rights Act 1998*, as well as concern over its potential effects on electronic commerce. This section of this paper concentrates on the objections made to the Draft Bill, and the question of whether the objections still apply to the *Regulation of Investigatory Powers Bill*.

[77] DTI, *Promoting Electronic Commerce*, July 1999, Cm 4417

A. Comparison between the *Regulation of Investigatory Powers Bill* and the Draft *Electronic Communications (EC) Bill*

Topic	Draft E C Bill	RIP Bill
Power to require disclosure of key	Cl 10	Cl 46 (redrafted)
Disclosure of information in place of key	Cl 11	Cl 47 (sub-cl (4) is new)
Arrangements for payments for key disclosure		Cl 48 (new)
Failure to comply with a notice	Cl 12+14	Cl 49 (redrafted)
Tipping-off	Cl 13	Cl 50 (redrafted)
Safeguards	Cl 15	Cl 51 (redrafted)

B. The problem of legislating for encryption

The background issue is that encryption is an important part of the techniques of electronic commerce, but is also useful to organised crime. The question is whether the legislative framework can encourage electronic commerce, but also prevent the techniques being abused by criminals.

A report by the Trade and Industry Select Committee explained the importance of encryption for the electronic commerce industry:

> **What is cryptography?**
> 9. When individuals and organisations communicate with each other they must trust the form and means of communication, in different ways. The parties to a communication might need to rely on:
>
> - the *authenticity* of the message, that it is sent by whoever purports to have sent it
> - the *integrity* of the message, that nothing has been omitted from or added to the message by anyone other than the purported sender
> - the *confidentiality* of the message, that no-one has seen the message other than those authorised to do so.
>
> Authenticity, integrity and confidentiality are not always required and, where they are needed, might not be guaranteed. A written signature can authenticate a letter, the integrity and confidentiality of which can be preserved by the use of a sealed envelope. Signatures can be forged and post intercepted, however, and written communications can be sent without a signature and without being sealed in an envelope and may still be trusted. Some communications, including commercial transactions, must be capable of *non-repudiation*. A contract will be invalid if one party to it can plausibly suggest that he or she never signed the contract, or agreed to a different set of terms than those later claimed by the other party. Confidentiality may also be a crucial requirement of many communications, including commercial transactions and dealings with official authorities.

10. The authenticity, integrity and confidentiality of electronic communications are important influences on the development of electronic commerce They may all be essential elements in persuading individuals and firms to enter into contracts and to interact with Government electronically. As with off-line communications, authenticity, integrity and confidentiality may not all be necessary elements of every electronic communication but, where they are required, two techniques are commonly employed:

- *electronic signatures*, which can authenticate the originator of an electronic communication and, in some cases, guarantee the integrity of the message sent
- *encryption*, to ensure the confidentiality of the communication.

Public-Key Cryptography

11. Although electronic signatures and encryption are distinct processes, they can be achieved by means of the same technology - public key cryptography. Each user of public key cryptography has both a private key, which is kept secret, and a public key, which can be published] The "keys" are long numbers which cannot be derived from each other, but which are related through the application of mathematical functions] Public-key cryptography works in the following way:

- if person A wishes to *encrypt* a message so that only person B may read it then A scrambles the text with B's public key. Only B's private key can be used to decrypt the message
- if person A wishes to *sign* a message then A's private key can be used to encrypt a digest of the message, which can be sent with the full message. B, or anyone else, can decrypt the digest with A's public key, thus proving that A was the originator. The integrity of a message can be demonstrated by comparing the decrypted digest with a digest of the text sent — any differences must have been created after the original text was signed off by A. These functions together ensure that A cannot repudiate the content of the message nor claim that he or she did not send it. This type of electronic signature is a digital signature.

12. Public-key cryptography's primary strength is that it can provide for confidentiality and non-repudiation over open networks - A and B do not need to meet to exchange keys or to establish each other's credentials before beginning to communicate. This is a significant advantage over other forms of cryptography which may require prior exchange of private keys (private-key cryptography). It can be seen that a document signed with a digital signature has an advantage over a conventionally signed one: the digital signature is intimately bound to the whole document whereas with a conventional multi-page document which is manually signed on the final page there is a greater possibility that, after signing, alterations may have been made on some of the earlier pages. Conversely, however, a document signed with a digital signature may also be less convincing to a recipient than one signed with a conventional signature because the linking of the signer's identity to the signature depends not on some unique physical quality - handwriting - but on a reliable publication which associates the public key with a specific person. Written

> signatures are tightly associated with people and weakly associated with documents, whilst digital signatures are tightly bound to documents and weakly bound to individuals (or identities).[78]

The DTI Consultation Paper, *Building Confidence in Electronic Commerce*, explained why encryption was considered to pose a serious threat to law enforcement:

> 49 A number of recent investigations into a variety of serious criminal offences in the UK have been hampered by the discovery that material which might otherwise assist the investigation, or be used in evidence, has been encrypted. The problem is increasing. Law enforcement agencies often try to "crack" the encryption key. Although this is occasionally possible after considerable effort and expense, it is likely to become increasingly difficult – if not impossible – as the technology develops.

It then gave examples:

- A case of attempted murder and sexual assault;
- Numerous cases of paedophiles using encryption;
- The Serious Fraud Office estimated that in approximately 50% of its cases, some form of encryption was encountered;
- Commercial interests faced a range of potential threats from improper use of encryption, including corporate espionage, insider theft, and attempts at extortion of money by placing enciphered viruses into computer systems.
- Terrorists were using encryption as a means of concealing their activities.[79]

Building Confidence in Electronic Commerce continued:

> 64 The Government proposes to establish a power to require any person, upon service of a written notice, to produce specified material in a comprehensible form or to disclose relevant material (e.g. an encryption key) necessary for that purpose. The ability to serve a written notice will be ancillary to existing statutory powers such as those contained in the *Interception of Communications Act 1985* and the *Police and Criminal Evidence Act 1984*. This means it will apply only to material which itself has been, or is being, obtained lawfully.
>
> 65 The new power will not make access to any encrypted communications or data lawful if it would otherwise be unlawful. For example, it is an offence to intercept communications on a UK public telecommunications network without a warrant issued by a Secretary of State. It will not be possible to obtain the Secretary of State's authorisation for access to encryption keys to decrypt unlawfully intercepted material.

---

[78] Trade and Industry Committee, *"Building confidence in Electronic Commerce": the Government's Proposals*, 12 May 1999, HC 187 1998-99, paragraphs 9-12

[79] DTI, *Building Confidence in Electronic Commerce*, 5 March 1999, Deposited Paper 99/494

The term "key escrow" describes a system in which the person who encrypts data has to leave the key with a third party. That was an early Government suggestion, but already by the time of the Draft *Electronic Communications Bill* the Government was proposing a more limited power whereby the authorities could demand the encryption key in certain circumstances.

C. The Select Committee Report on Part III of the Draft *Electronic Communications Bill*

As part of the pre-legislative scrutiny, the Trade and Industry Select Committee produced a Report on the Draft *Electronic Communications Bill*.[80] The Committee did not share the fears expressed elsewhere over the human rights implications of the Bill. The Government Response to the encryption part of that report contains the Committee's recommendations, along with the Government's responses:

> *(i) We have seen nothing that would substantiate some hysterical comment to the effect that the Government's proposed new power to require decryption represents a major assault on our rights; subject to our recommendations below, we see no reason to depart from our earlier conclusion that the proposed new power would prove a useful addition to the armoury of the law enforcement agencies. If Home Office Ministers wish to proceed with part III of the draft Bill then they must explain in more detail than hitherto why the proposed new power should be introduced with such urgency.*
>
> The Government welcomes the Committee's conclusion that, subject to the recommendations contained in its report, the proposed new decryption powers would prove useful to law enforcement. The Government listened and reflected on how best to take forward the proposals set out in the draft Electronic Communications Bill and, as the Committee will know, decided to legislate separately during the current session of Parliament to modernise law enforcement powers in this area. The Home Office will bring forward legislative proposals, together with those for updating the law on the interception of communications and other intrusive investigative techniques, in the forthcoming Regulation of Investigatory Powers (RIP) Bill.
>
> *(j) We have heard significant expressions of dissatisfaction with the present regime for interception of communications, particularly concerning the lack of judicial oversight including from the Data Protection Registrar in evidence to us in March 1999. We would expect these concerns to be addressed fully by the Government when it responds to the consultation exercise on the future of the interceptions regime. We also recommend that the Government seek ways of alleviating the cost burden on smaller internet service providers of extending the scope of the interception of communications regime, and requiring decryption of intercepted encrypted messages, if necessary, by ensuring that the burden is shared on a proportionate basis.*
>
> In the consultation paper outlining plans for updating the law on the interception of communications, the Government proposed to continue with the long established principle of

---

[80] Trade and Industry Committee, *Draft Electronic Communications Bill*, HC 862 1998-99

Secretary of State authorisation of interception. Alternative options had been examined but on balance, the Government was not persuaded that the current practice should be altered. The Government has considered carefully all the responses received to the interception consultation exercise (details of which have now been published on the Home Office website) but remains of the view that the power to authorise interception warrants should continue to be vested in the Secretary of State. There will continue to be an independent Commissioner with responsibility for overseeing the Secretary of State's use of the power of interception. The Government believes that the Commissioner fulfils an important and effective oversight role.

As regards costs, large parts of the telecommunications industry are covered by the current interception legislation and will incur little or no extra cost under the proposals to update the law. The Government is consulting in order to get a balanced view from across the industry, including the Internet Service Provider community, of what constitutes a reasonable intercept requirement. There is no intention of imposing burdens on industry which are anything other than reasonable.

(k) We recommend that the legislation address the issue of the extent to which all or some non-Home Office police forces should be given the powers and duties proposed in part III of the draft Bill.

The Government is looking carefully at whether, and how best, to cover non-Home Office police forces as regards the proposed decryption powers in the forthcoming RIP Bill.

(l) We recommend that the Government make available to Parliament before second reading of the Bill the criteria concerning the circumstances in which a written notice for decryption will be able to require the production of a private key.

The Government will seek to make available to Parliament, during the passage of the forthcoming RIP Bill, the criteria concerning the circumstances in which decryption keys rather than an intelligible version of protected data may be required. It is envisaged that this will be covered in the proposed Code of Practice. The Government would also reiterate the response made to the Committee's previous query on this point - it is envisaged that the disclosure of an intelligible version of protected data in response to a decryption notice will be sufficient in most cases.

(m) We recommend that the legislation explicitly addresses the question of the exemption of privileged material from the scope of written decryption notices.

The proposed new decryption powers will not undermine safeguards in existing legislation governing access to privileged material. For example, under the Police and Criminal Evidence Act 1984 (PACE), the authority of a Circuit Judge is required for access to e.g. legally privileged or journalistic material. It is proposed that use of the decryption power in such circumstances will require the same level of authorisation.

(n) We recommend that the Government give some indication as to how it is envisaged that those served with written notices requiring plain text or encryption keys can successfully demonstrate that they cannot comply with the notice. We agree with the underlying aim of the tipping-off offence, but seek assurances that it will be used against only those people who

deliberately and intentionally seek to subvert the work of the law enforcement agencies. We recommend that, once the legislation is in force, the Government keeps under review the penalties for the offences of tipping-off and failure to comply with a written notice.[81]

The Government recognises that the proposed offences contained in the draft Bill have aroused much comment from interested parties. The construction of the relevant draft Clauses is being examined carefully in the light of the responses to the consultation exercise on the draft Bill. The Committee may be assured that it is the Government's intention that the new offences seek to target the criminal or their associates, not the legitimate or innocent user of encryption technologies. The penalties for the proposed offences will be kept under review once the legislation is in force.

(o) The proposed code of practice may prove toothless. We recommend that:
- any person exercising or performing any power or duty under part III of the legislation should have an enforceable duty to follow the requirements of the proposed code of practice at all times

- procedures are established to report, independently monitor and publish details of breaches of the proposed code of practice, possibly through the good offices of the proposed Commissioner.

The Government is considering carefully how the proposed statutory Code of Practice is to be best operated. The view of the Committee, as well as other commentators on the draft Bill, will be taken into account in bringing forward the RIP Bill.

Legislation
(cc) Having certified that legislation does not contravene the European Convention on Human Rights, Ministers must be able to demonstrate, when challenged, that this is indeed the case. We recommend that the Government publish a detailed analysis to substantiate its confidence that part III of the draft Bill does not contravene the European Convention on Human Rights, dealing with the points made to the contrary.

The Government has every intention of ensuring that all the provisions of the forthcoming RIP Bill are ECHR compatible. And the Government will be very happy to explain why it believes the provisions to be ECHR compatible when faced with specific argument to the contrary. All such discussion should take place against the backdrop that any challenges to legislation on these grounds will rely on the specific nature of the case in question. Therefore, these issues are hard to deal with comprehensively in advance of any particular challenge.[82]

---

81 This is discussed in Part III E of this paper

82 Trade and Industry Committee, *Further Government Observations on the Fourteenth Report from the Trade and Industry Committee (Session 1998-99) on the Draft Electronic Communications Bill*, 1 February 2000, HC 237, 1999-2000

D. Human Rights Issues in the two Bills

The Foundation for Information Policy Research (FIPR) and the human rights organisation *Justice* obtained a legal opinion from Jack Beatson QC and Tim Eicke, arguing that Part III of the draft *Electronic Communications Bill* would not have complied with the *Human Rights Act 1998*.[83] Their concerns related to the power in that Bill to require the disclosure of a key to encrypted material and to the privacy implications of having one's encrypted messages read by a third party.

1. Power to require disclosure of key

Clause 10 of the draft *Electronic Communications Bill* would have enabled properly authorised people to require the disclosure of a key to encrypted material. Clause 46 of the RIP Bill covers much the same ground.

Clause 10 in the Draft *Electronic Communications Bill* was controversial, particularly on grounds stated by the British Computer Society (BCS):

> Clause 10(2). The BCS is concerned that a defendant has to prove beyond all reasonable doubt that they do not have the key. The BCS recommends that it should be up to the authorities to prove that beyond reasonable doubt that a person has the key before it is mandatory for the person to hand over the key.[84]

The legal opinion obtained by FIPR and Justice went further, stating that Clause 10(2), taken together with the power in Clause 12 to impose a penalty for failure to comply with a notice under Clause 10, would be likely to infringe the European Convention on Human Rights. The authors argued that it would be likely to infringe the right in Article 6(1) of the Convention to a fair hearing and the presumption of innocence in Article 6(2).[85]

In Clause 10 of the Draft *Electronic Communications Bill*, the test for whether someone could be required to disclose a key was: "If it appears to any person with the appropriate permission…that a key to the protected information is in the possession of any person…"
Clause 46 of the *Regulation of Investigatory Powers Bill* replaces that test by: "If any person with the appropriate permission…believes, on reasonable grounds that a key to the protected information is in the possession of any person…" In other words, in the *Regulation of Investigatory Powers Bill* the test contains an objective element, whereas the earlier version was purely subjective.

There is also a change in the section dealing with failure to comply with a notice. In the draft *Electronic Communications Bill* Clause 12: "A person is guilty of an offence if he fails to comply, in accordance with any section 10 notice, with any requirement of that notice to

---

83 www.fipr.org/ecomm99/ecommaud.html, 15 February 2000
84 British Computer Society, *A Response to the Electronic Communications Bill of 23 July 1999*, paragraph 22
85 www.fipr.org/ecomm99/ecommaud.html, 15 February 2000

disclose a key to protected information". The Summary of Responses to *Promoting Electronic Commerce* stressed concern in this area:

> Right across the whole spectrum of responses, it was feared that the phrasing of the offence of "failing to comply with a notice", and its statutory defences, would be held to reverse the burden of proof – all the more serious since the requirement on the defence would, in effect, be to prove non-possession. Defining the offence as something like "failing to deliver a key (or plaintext) to which he had access" was seen as preferable.[86]

Clause 49 of the *Regulation of Investigatory Powers Bill* adds the extra necessary condition that: "he is a person who has or has had possession of the key".

The FIPR argues that the Human Rights problems with the Draft Bill have not been removed by the redrafting of the *Regulation of Investigatory Powers Bill*:

> The Home Office have made limited changes that amount to window-dressing, but the essential human rights issue remains:
>
> > (Clause 46): authorities must have "reasonable grounds to believe" the key is in possession of a person (previously it had to "appear" to authorities that person had a key). This replaces a subjective test with one requiring objective evidence, but leaves unaffected the presumption of guilt if reasonable grounds exist.
> >
> > (Clause 49): to prove non-compliance with notice to decrypt, the prosecution must prove person "has or has had" possession of the key. This satisfies the objection to the case where a person may never have had possession of the key ("encrypted e-mail out of the blue"), but leaves unchanged the essential reverse-burden-of-proof for someone who has forgotten or irreplaceably lost a key. It is logically impossible for the defence to show this reliably.[87]

Those who use encryption stress the risk that they might have lost or forgotten the key. A key is typically a 128 bit number, that would be stored on a computer and the user of encryption would typically have a phrase that would enable him to reach the correct file to find the number. If that phrase is forgotten, then the user of encrypted material would be unable to provide the key, but would not be able to prove that he no longer had it.

The Civil Rights organisation *Liberty* also raised concerns:

> We consider that the Government has failed to demonstrate any need for a new regime of compulsory access to decryption keys. The parties to an electronic communication remain free to encrypt "at source" themselves. There is no technical

---

[86] DTI, *Summary of Responses to Promoting Electronic Commerce*, 1 November 1999, paragraph 23

[87] FIPR, *UK Publishes "Impossible" Decryption Law*, 10 February 2000

> necessity that encryption keys should be held by anyone but the parties. Persons who intend serious wrongdoing are precisely those most likely to take advantage of that fact. So the Bill will enable serious infringements of privacy for no worthwhile gain. That flatly conflicts with the principle of proportionality. The reference to proportionality in clause 46(2) cannot meet this fundamental objection.
>
> If a case of need can be made in principle for access to encrypted information, it is unlikely to support the draconian step of requiring supply of decryption keys. PACE 1984, Schedule 1 para. 5, provides that a judge's order for disclosure of information held on computer requires its supply "in a legible and visible form". That provision could readily be adapted to supplement other investigatory powers.
>
> If Part III is to remain in broadly its present form, we have the following concerns (among others):
>
> - Authorisation should generally be by way of application to a judge on notice to the key holder.
>
> - The clause 49(1) offence is too onerous and improperly casts the burden of proof on an accused who, by definition, is not the target of the investigator's suspicions. The basic obligation should be take all practicable steps to disclose a key (or plaintext) in one's possession when the authorisation is served. The prosecution should have to prove non-compliance with that obligation in the ordinary way.
>
> - The tipping off offence (clause 50) is a serious one (subs. (3)). Several of its provisions improperly cast a burden of proof on the accused.[88]
>
> - There should be a requirement (and corresponding exemption from clause 50) for after-the-event notice to the parties whose data security has been compromised by the disclosure of a key.[89]

The problem of security of keys was noted in a second briefing by the FIPR:

> The Government has not considered the problems and costs of handling decryption keys when it takes new powers to seize them, says a nine-page report[90] released today by the influential Internet policy think-tank the Foundation for Information Policy Research. If the keys were disclosed, or even stolen from the authorities that had seized them, then this could result in extreme risks to physical safety and financial security. The new powers are in the controversial Regulation of Investigatory Powers (RIP) Bill that receives its second reading in the Commons on March 6th.
>
> The report analyses the Government's proposals for safeguarding seized keys, finding that they take no account of the technical security measures used by government to

---

88 This is discussed in Part III E of this paper

89 Liberty, *Regulation of Investigatory powers Bill: Second Reading Briefing*, February 2000

90 http://www.fipr.org/rip/RIPGAKBG.pdf

> protect their own keys, and make no provision whatsoever for keys seized under RIP to enjoy comparable levels of protection. Hundreds of public authorities are able to demand keys (set out over five pages in Schedule.1), but none are required to take concrete security precautions on behalf of those who are forced to reveal their keys – whether suspect or innocent parties in an investigation.
>
> The report concludes that the necessary protection measures will be very costly to implement and are hence likely to place a very high burden on UK taxpayers if the interests of the owners of seized keys are to be fully respected. It concludes that there is a danger that the costs of such measures will not be met and in consequence those who have their keys seized will sometimes face extreme risks to their safety and security.[91]

The Data Protection Commissioner has criticised the wide definition of a "key" in the Bill:

> The Commissioner is concerned that the proposed legislation is currently drafted in such a way that Part III of the Bill has implications not just for encrypted personal data, but for wider categories of electronic data.
>
> Part III of the Bill provides powers for law enforcement agencies and others to require the disclosure of any 'key'. This term is defined under s 52 of the Bill as any key, code, password, algorithm or other data which allows access to electronic data or which facilitates the putting of the data into an intelligible form. This wide definition means that mechanisms such as 'passwords' and codes used for gaining access to a computer room might be caught by the Bill.
>
> In the original consultation document it was made clear that the aim of the Government was to address the problem of lawful access to encrypted information and the Commissioner is unclear why the scope of the legislation has been extended to cover a wider range of protected data.
>
> The value of the encryption process is to safeguard confidential or sensitive information, access to which could have serious repercussions for the privacy of the individual to whom the data relate.
>
> In the case of encrypted data the Bill, as currently drafted, makes it unlikely that individuals will be informed where the integrity of their private keys has been jeopardised and they may continue to use these keys without being aware that their security has been compromised. Third parties whose personal data forms part of any protected electronic information may also be unaware of the risks posed to their data.[92]

---

91 FIPR, *RIP bill leaves seized keys vulnerable*, 28 February 2000

92 Data Protection Commissioner, *Response of the Data Protection commissioner to the Government's Regulation of Investigatory Powers Bill*, March 2000

The Commissioner also noted the danger of the falsification of a notice under Clause 46 requiring the handing over of a key, particularly since that Clause did not require the notice to be made in writing. He argued that stronger safeguards were required than those in the Bill:

> A warrant should also be required for access to protected electronic data. The Commissioner is concerned to note that the Bill appears to allow access to protected information without a warrant by the police, Customs and Excise or Her Majesty's forces.
>
> Access to protected electronic data should be subject to safeguards and controls which are no less stringent than those applying to the interception of the original communications. If parties have chosen to encrypt the communications it is presumably because they wish to keep them secret. A breach of this secrecy may have serious implications not only for the parties communicating but also for any third parties whose information forms part of the text of the encrypted material. Consequently, access to these communications should be subject to restrictions which are if anything more rather than less onerous than those applying to plain text communications.
>
> A clause 46 notice should only be served where a judge or another independent authority has ruled that there are sufficient grounds for approving its issue. Whether or not access can be required should be subject to a prejudice test similar to that set out in s.29 of the Data Protection Act 1998.[93]

Although similar issues are arising in many countries, the requirement to disclose a key is not a power in the law of other major IT countries such as the USA, France or Germany. One possible reason for that is the difficulty of proving one way of the other whether somebody has the key. It would be very hard for the authorities to prove that an individual has the key, but the original attempt to reverse the burden of proof, leaving him to prove that he did not have the key, presented insuperable human rights problems. However, this is an area that is changing fast. Only in the past two years or so has the USA abandoned the attempt to impose key escrow, and other countries have followed. If the British Government managed to introduce a power to require the disclosure of a key, then other countries might introduce similar requirements.

2. Privacy

The FIPR legal opinion argued that the requirement to hand over a key to encrypted material conflicted with the right to privacy in the European Convention on Human Rights:

> Especially where the private key is handed over, the law enforcement agencies will be able to decrypt and read any message received by the addressee of the notice, irrespective of whether it is covered by legal professional privilege or not. Only once

---

[93] ibid

> a message has been read will it be clear whether the material contained therein is privileged in any way or not. There is nothing in the draft Bill that provides for supervision by an independent judge in relation to the decryption of intercepted material.[94]

The *Regulation of Investigatory Powers Bill* extends the safeguards in two ways. First, Clause 51(c) lays down the general duties of the Secretary of State and others to ensure that the process of obtaining the key and decryption are properly carried out. Clause 15 of the Draft Bill covered much the same ground, but Clause 51(c) contains an extra requirement;

> that, having regard to those matters, the use and any retention of the key are proportionate to what is sought to be achieved by its use and retention.

The term "those matters" refers to "the uses to which the person using the key is entitled to put any protected information to which it relates and to the other circumstances of the case".

The second added safeguard comes in the duties of the Covert Investigations Commissioner, which include keeping under review:

> 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

Therefore the privacy objections to the Draft Electronic Communications Bill do not necessarily apply to the *Regulation of Investigatory Powers Bill*.

E. Objections from the Electronic Commerce Industry to Part III of the Draft *Electronic Communications Bill*

The industrial objections to the encryption part of the Draft *Electronic Communications Bill* have a very different status from the human rights objections. The human rights objections are specific and would be decided ultimately in a Court of Law. The objections from the electronic commerce industry might result in firms disliking the legislative environment in the United Kingdom and deciding to do business elsewhere instead. The Summary of Responses to *Promoting Electronic Commerce* noted general concerns in the world of electronic commerce:

> Several respondents suggested that the impact of the Bill could go beyond its stated limited objective of maintaining the effectiveness of existing law enforcement powers. A common and weighty view was that whilst occasional warranted access by Law Enforcement Agencies to plaintext seems reasonable (with proper safeguards), the possibility of their access to keys seriously undermines e-commerce and the integrity of service providers, as well as causing huge potential costs in global key revocation and change; if it must happen at all it should be exceptional, specially

---

[94] www.fipr.org/ecomm99/ecommaud.html, 15 February 2000, paragraph 20

> justified and/or warranted, specially controlled, and with adequate compensation. However, the principal thrust of the Bill as drafted was perceived as being that disclosure of keys could become the norm.[95]

It is unclear exactly which aspect of the draft *Electronic Communications Bill* gave the idea that disclosure of keys could become the norm, and therefore it is unclear whether the *Regulation of Investigatory Powers Bill* will give rise to the same concerns. Until recently, the use of encryption was uncommon, partly because the best encryption technology could not be exported from the USA because of export controls. That restriction no longer applies, since January 2000, and encryption may become a routine aspect of electronic commerce. The new Microsoft package Windows 2000 contains a strong encryption facility.

If the use of encryption becomes widespread, then the possibility also arises that the requirement to disclose keys could be used not just for the detection of an occasional drugs or paedophile gang, but for a much wider range of police investigations.

The submission by Microsoft to the consultation begun in July 1999 by the publication of *Promoting Electronic Commerce* explains a related area of concern:

> However, the Government's decision not to impose key escrow in the draft Bill is threatened by the Home Office's consultation document *Interception of Communications in the United Kingdom* (the "IOCA Consultation"). This consultation is silent as to whether communications service providers (CSPs) would be obligated to provide interception of communications in a readable (or otherwise decrypted form) or simply provide access to the "raw" (or un-decrypted) communication. If CSPs were obliged to provide unencrypted data, this might effectively force CSPs to require their customers to use key escrow or third-party key recovery systems. Even if key escrow or third-party key recovery are not mandated, the IOCA Consultation proposes requiring communications systems be designed in advance to allow for interception for the purposes of understanding a communication. This proposal could be construed as requiring CSPs to design their systems to allow for interception at a point prior to encryption or after decryption in respect of any particular portion of the message route. While conceptually simple, this idea will not work in practice, as it is technically infeasible; further, it poses the same problems as key escrow. Therefore, Microsoft urges the Government to be vigilant in ensuring that key escrow, with all of its negative effects, is not introduced, through the back door, within the bill that will result from the IOCA Consultation.[96]

The *Regulation of Investigatory Powers Bill* does not impose an obligation on the suppliers of communications or cryptography services to supply either a key or encrypted information. Clause 49 makes it clear that the offence of failing to comply with a section 46 notice to supply either a key or encrypted information only applies to a person who has or has had

---

95 DTI, *Summary of Responses to Promoting Electronic Commerce*, 1 November 1999, paragraph 20

96 *Microsoft's Response to the Government's Consultation Document: Promoting Electronic Commerce*, October 1999

possession of the key. That provision would exclude any danger of a supplier of cryptography services being expected to keep all the keys in case of a challenge by the law enforcement authorities.

The Summary of Responses to the Consultation also noted further concerns:

> There was a view that Part III does not take enough account of the technical and operational difficulties of its implementation. Very substantial costs were foreseen, as well as situations in which some technical or operational infeasibility could cause serious misunderstandings, for example between service providers and Law Enforcement Authorities. The attempt to restrict disclosure of keys to those used for encryption was questioned on the grounds that dual-use keys are common: the possibility of their compromise would affect confidence in the reliability of electronic signatures etc.[97]

The *Regulation of Investigatory Powers Bill*, in Clause 48, allows for payment arrangements to be made to compensate those required to disclose information under a section 46 notice. The other concerns from the electronic commerce industry appear to remain, however. They may, however, be answered by the codes of practice for which provision is made in Clause 62 of the Bill.

1. Tipping-off

It is widely held that the decryption of criminal communications would become relatively ineffective as a tool of law enforcement agencies if the criminals knew that their messages were being decrypted. Therefore both the draft *Electronic Communications Bill* and the *Regulation of Investigatory Powers Bill* provide for an offence of "tipping off". This allows an order to provide a key to encrypted material to include a requirement that "the giving of the notice, its contents and the things done in pursuance of it" be kept secret. Disclosure of that information would be an offence with a penalty of up to five years in prison. Several specific defences are listed in Clause 13 of the draft Bill. Basically, it would be a defence: if the disclosure was entirely effected by the operation of software; if the disclosure was made to a professional legal adviser by a client, or vice versa, or by a professional legal adviser in connection with court proceedings; if the disclosure was authorised; or if the person did not know that the direction contained a secrecy provision.

The original provisions were unpopular, as noted in the summary of replies to the consultation exercise:

> There was much objection to the tipping-off offence. Service providers and others felt that in practice it would "force them to lie"; lawyers felt that it would be unenforceable. A major service provider wanted expansion of the software defence to embrace disclosures effected by hardware and operational routines; law

---

[97] DTI, *Summary of Responses to Promoting Electronic Commerce*, 1 November 1999, paragraph 22

> enforcement agencies suggested that it be replaced by a more general "reasonable excuse" defence.[98]

Clause 50 in the *Regulation of Investigatory Powers Bill* contains the tipping-off offence in very similar terms to the offence in Clause 13 of the draft Bill. The specific defences are left the same, and there is no "reasonable excuse" defence. The change comes in a restriction, in sub-clause 2, on what a section 46 notice can contain:

> A section 46 notice shall not contain a requirement to keep anything secret except where the key to which it relates is a key to protected information which –
>
> (a) has come into the possession of the police, the customs and excise or any of the intelligence services, or
> (b) is likely to come into the possession of the police, the customs and excise or any of the intelligence services,
>
> by means which it is reasonable, in order to maintain the effectiveness of any investigation or of investigatory techniques generally, or in the interests of the safety or well-being of any person, to keep secret from a particular person.

This looks like part of a general move to limit the use of the powers in part III of the Bill, rather than to allow the powers to be used extensively, in which case there would be potential disruption of the electronic commerce industry.

If the electronic commerce companies dislike the measures in the Bill, they might choose to do business elsewhere. However, there are other possible ways of concealing information. There is a technique called steganography, which has legitimate uses in the music industry to trace the origins of pirate copying. However, it could also be used to conceal information in a way that could circumvent to requirement to provide a key to encrypted material. If the electronic commerce industry finds itself burdened by excessive requirements to disclose keys, then it could use steganography to protect information.[99]

On the other hand, law enforcement agencies might be able to trace the pattern of electronic communications, even without reading the messages. For example, they could build up a picture by studying the origins of the e-mails received by suspected drugs dealers, or check which web sites had been accessed by a suspect. Similar methods in relation to billing information produced by telephone companies have been in use for some time.[100] Such searching might be defeated by software that would preserve anonymity. There is a constant struggle between new electronic methods to discover more information about from internet and other methods designed to conceal the information.

---

[98] DTI, *Summary of Responses to Promoting Electronic Commerce*, 1 November 1999, paragraph 24

[99] According to Grant Bowden of the FIPR

[100] see part II of this paper

IV Reactions to the Bill

One of the contentious issues raised by the Bill is the scope it gives to the police and Customs and Excise to obtain communications data - **Clause 21**, for example, lists a wide range of situations in which communications data might be obtained. A recent article in the *Guardian* discusses some of the arguments surrounding the Bill:[101]

> **Ministers seek wide bugging powers**
>
> Sweeping powers allowing the intelligence services and other government agencies to conduct covert surveillance, including bugging phones and property, were proposed by the government yesterday.
> ... But critics of the regulation of investigatory powers bill said the new power could be open to abuse.
> Charles Clarke, the home office minister, said the measure would allow the police and other agencies to keep up with the sophisticated technology used by criminal gangs.
> It would also place covert activities already undertaken by the security and intelligence services on a regulated, statutory basis, to make them compatible with the European convention on human rights, which will be incorporated into English law on October 2.
> There were some 'extremely fuzzy' areas which could now be open to challenge under the convention, said Mr Clarke.
> The bill covers a wide range of intrusive surveillance techniques, including systematic targeting of an individual over a period of time in order, as the home office puts it, 'to obtain a picture of his life, activities and his associates'.
> It includes the bugging of private property and cars, and the use of 'covert human intelligence sources' - informants or undercover officers.
> It will include activities well beyond those of the security and intelligence services and the police. Ministers will be able to issue orders allowing many other agencies to undertake covert surveillance.
> They include the departments of health and social security, the ministry of agriculture, and the department of trade and industry as well as local authorities.
> While the bill says that warrants for intercepting communications would still be signed by cabinet ministers, authorisation for other forms of surveillance would be given by senior police officers or even local authority officials.
> Mr Clarke concentrated on what he called 'sophisticated international organisations' with access to the most powerful technologies. Paedophile networks, for example, were using encryption to protect material on computers. The home office, meanwhile, said that phone tapping had enabled customs officers to seize 1.25 tonnes of class A drugs during a recent 12 month period.
> The bill sets up the post of a covert investigations commissioner to monitor the issuing of warrants and a new complaints tribunal.

[101] 'Ministers Seek Wide Bugging Powers' *The Guardian* (Richard Norton-Taylor) 11 February 2000

> Liz Parratt, for Liberty, the civil rights group, said that the European court of human rights had always emphasised the importance of prior judicial sanction for warrants rather than authorisation by a politician or police officer.
> 'And in their current form powers to recover encryption keys risk reversing the burden of proof. But, overall, efforts to introduce a consistent regulatory framework in this area should be welcomed.'

The Foundation for Information Policy Research's Press Notice of 10 February 2000 argued that the Bill was no improvement on the draft *Electronic Communications Bill*.[102]

> **UK PUBLISHES "IMPOSSIBLE" DECRYPTION LAW**
>
> Today Britain became the only country in the world to publish a law which could imprison users of encryption technology for forgetting or losing their keys. The Home Office's Regulation Of Investigatory Powers (RIP) bill has been introduced in Parliament: it regulates the use of informers, requires Internet Service Providers to maintain "reasonable interception capabilities", and contains powers to compel decryption under complex interlocking schemes of authorisation.
>
> Casper Bowden, director of Internet policy think-tank FIPR said, "this law could make a criminal out of anyone who uses encryption to protect their privacy on the Internet. The DTI jettisoned decryption powers from its e-Communications Bill last year because it did not believe that a law which presumes someone guilty unless they can prove themselves innocent was compatible with the Human Rights Act. The corpse of a law laid to rest by Stephen Byers has been stitched back up and jolted into life by Jack Straw."

A recent article in the *Daily Telegraph* also referred to the concerns of civil liberties campaigners. The article has been edited for length:[103]

> **Bill revives attack on privacy**
>
> Civil liberties and privacy campaigners are up in arms over a fresh attempt to bring in measures that would give law enforcement agencies the right to demand encryption keys from people using cryptography to protect data.
> The Regulation of Investigatory Powers (RIP) Bill, published last week, contains updates to existing police powers and includes the clauses regarding cryptography that were struck from the Electronic Communications Act.
> The Bill is intended to update or supersede a number of pieces of existing legislation, including the Police and Criminal Evidence Act and the Interception of Communications Act. Among other surveillance powers, the Bill gives the Secretary of State the right to require internet service providers and other telecommunications or postal services providers to ensure that their networks be tappable. Individuals will

---

[102] *Flash FIPR Press Release on the Regulation of Investigatory Powers Bill:* FIPR 10 February 2000
[103] 'Bill revives attack on privacy' *Daily Telegraph* 24 February 2000

have to produce their decryption keys when given notice to do so by law enforcement, and a new offence called 'tipping-off' makes it a crime to tell anyone other than a legal adviser that such a notice has been issued.

Organisations concerned with civil liberties and privacy rights, such as Privacy International, Liberty, the Foundation for Information Policy Research (FIPR), and the Campaign Against Censorship in Britain all criticise the Bill as breaching human rights.

Caspar Bowden, executive director of FIPR, said: 'This law could make a criminal out of anyone who uses encryption to protect their privacy on the internet.'

In addition, he noted: 'There is the issue of access to traffic data, which at the moment is pretty much unlimited. There is no control or independent oversight of that, and it's a really worrying new technique of mass surveillance - a big database of who's talking to whom, what they're interested in, which organisations they're members of, and so on.'

…

The FIPR, which co-sponsored the earlier human-rights audit [of the Electronic Communications Bill] with the legal human rights organisation Justice, believes it inevitable that the new legislation will be challenged on the same grounds.