RP02/04-05

Regulation of Interception of Communications in Selected Jurisdictions

2 February 2005

Prepared by

Thomas WONG

Research and Library Services Division
Legislative Council Secretariat

5th Floor, Citibank Tower, 3 Garden Road, Central, Hong Kong
Telephone : (852) 2869 9621
Facsimile : (852) 2509 9268
Website : http://www.legco.gov.hk
E-mail : library@legco.gov.hk

C O N T E N T S

Acknowledgements

We sincerely acknowledge the kind assistance given to us by many people in the preparation of this research report. In particular, we would like to express our gratitude to the following individuals/organizations for providing us with valuable information:

Ms Chan, Becky, Assistant Legal Liaison Officer, Federal Bureau of Investigation, Department of Justice, the United States;

Mr Cooper, Tony, Crime Reduction and Community Safety Group, the Home Office, the United Kingdom;

Mr Cranmer, Frank, Principal Clerk of Bills, House of Commons, the United Kingdom;

Mr Fitzgerald, David, Director of People Strategies, House of Representatives, the Parliament of Australia;

Ms Laurant, Cedric, Policy Counsel, Electronic Privacy Information Center**,** the United States;

Security Bureau, the Hong Kong Special Administrative Region Government;

Ms Trigeiro-Pabst, Linda M., Executive Secretariat Office, Federal Bureau of Investigation, Department of Justice, the United States of America;

Web Team, the Security Service, the United Kingdom.

Executive Summary

1. This report studies the statutory regulatory regimes of interception of communications in the United Kingdom (UK), the United States (US) and Australia. They are examined in 10 aspects: legal framework; authorities responsible for issuing warrants, application procedures; grounds on which warrants are issued; duration, termination and renewal of warrants; lawful interception without a warrant; internal safeguard measures; external safeguard mechanisms by the executive branch, the judiciary, the legislature and the public; limit of executive discretion in bringing laws into operation; and legislative amendments in relation to the "911" incident and the development of communications technology.

2. In the UK, interception of communications is principally regulated by a statute known as the Regulation of Investigatory Powers Act 2000. Only the heads of law enforcement or security agencies, or their representatives, are eligible to apply for interception warrants. These warrants are issued by the Secretary of State. Warrant applications must meet the tests of necessity and proportionality. The effective period for all new warrants is the same, but may vary after renewal, depending on their purposes. Intercepted materials are not admissible as evidence in legal proceedings, except in limited circumstances. The use of interception powers is monitored by the Interception of Communications Commissioner whose annual reports to the Prime Minister are tabled in Parliament and then made available to the public. The expenditure, administration and policies relating to interceptions for national security purposes are monitored by a statutory parliamentary committee. Members of the public can lodge complaints with the Investigatory Powers Tribunal, which has power to cancel warrants and award compensation. In recent years, legislative amendments have been introduced to enhance the implementation of the interception law and combat terrorism.

3. In the US, interception of communications is mainly regulated by three statutes. Title III of the Omnibus Safe Streets and Crime Control Act 1968 (Title III) regulates interception of the contents of communications for law enforcement purposes. The Foreign Intelligence Surveillance Act of 1978 (FISA) regulates interception of the contents of communications of foreign powers and their agents within the US. The Pen Registers and Trap and Trace Devices chapter of Title 18 (the Pen/Trap statute) regulates interception of non-content information of communications. Interception orders under the three statutes are all issued by Judges. Under Title III and FISA, court order applications must be authorized or approved by high-level judicial officials, and the issue of court orders must meet the "probable cause" test. The Pen/Trap regulatory system is less demanding, under which a court order is issued as long as the information to be intercepted is relevant to criminal investigation. The effective period for FISA orders is the longest, and Title III orders the shortest. Evidence gathered lawfully may be used in legal proceedings. The head of the Department of Justice is required by all three interception statutes to submit annual reports to Congress, but the information disclosed is different among them. Intercepting agencies are accountable to parliamentary committees. After the "911" incident, significant amendments to the three interception statutes have been made by the Uniting and Strengthening of America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act to increase the government's interception powers.

4. In Australia, interception of communications is principally regulated by a statute known as the Telecommunications (Interception) Act 1979. National security warrants, the application of which must be made by the Director-General of Security, are issued by the Attorney-General. The reasons for issuing such warrants are not necessarily related to particular offences. The application for law enforcement warrants must be made by eligible authorities, and such warrants are issued by Judges or nominated members of a tribunal for the investigation of specified offences. The maximum effective period for national security warrants is twice as long as that for law enforcement warrants. Lawfully intercepted information is admissible as evidence in exempt proceedings or defined circumstances or for permitted purposes. The Ombudsman is empowered to inspect the records of law enforcement warrants. The Attorney-General is required to table annual reports in the Australian Parliament giving details of telecommunications interceptions for law enforcement purposes. Law enforcement and security agencies are accountable to two statutory parliamentary committees. There have been several significant legislative amendments enacted by the Australian Parliament, most of which are part of the Australian government's measures against terrorism.

5. The Analysis focuses on comparing the various features of the interception warrant systems in the three selected jurisdictions. The comparison is made with reference to the Telecommunication Ordinance, which currently regulates interception of communications in the Hong Kong Special Administrative Region, the Interception of Communications Ordinance, which was enacted in June 1997 but has not been brought into operation by the Government, and the White Bill on interception of communications, which was published by the Government in February 1997 for public consultation but has not been introduced into the Legislative Council.

Regulation of Interception of Communications in Selected Jurisdictions

Chapter 1 - Introduction

1.1 Background

1.1.1 At the meeting of the Panel on Security on 2 April 2004, the Panel requested the Research and Library Services Division (RLSD) to conduct a research on the regulation of interception of communications in overseas jurisdictions. The research is to assist the Panel in deliberating matters relating to the Administration's current review of the Interception of Communications Ordinance (IOCO), which was enacted on 28 June 1997 but has not been brought into operation. At the meeting of the Panel on 13 May 2004, the proposed outline on the research was endorsed. Members requested RLSD to incorporate in the research a study of the legislative amendments in other jurisdictions arising from the "911" incident and the development of communications technology, and an analysis of whether interception of communications in other jurisdictions requires a court warrant or an executive order.

1.2 Scope of research

1.2.1 This research covers the statutory regulation of interception of communications in the following places:

(a) the United Kingdom (UK);

(b) the United States (US); and

(c) Australia.

1.2.2 These three common law jurisdictions are chosen not only because each of them has certain distinctive regulatory elements on interception of communications, but also because they have introduced in recent years significant legislative amendments impacting on individual privacy and interception power of law enforcement agencies. In particular, in the UK, an act has been enacted to create a new framework for interception of communications. The US has also enacted an act to enhance the surveillance procedures regarding terrorist activities. In Australia, the telecommunications interception legislation has been amended to cover terrorist acts that can be investigated with interception warrants.

1.2.3 The proposed selection of jurisdictions is consistent with the scope of a report published by the Law Reform Commission of Hong Kong in 1996 and entitled "*Privacy: Regulating the Interception of Communications*" in which the experiences of the three jurisdictions were discussed.

1.2.4 The regulation of interception of communications is examined in the following aspects:

(a) legal framework;

(b) authorities responsible for issuing warrants;

(c) application procedures;

(d) grounds on which warrants are issued;

(e) duration, termination and renewal of warrants;

(f) lawful interception without a warrant;

(g) internal safeguard measures;

(h) monitoring mechanisms by the executive branch, the judiciary, the legislature and the public;

(i) limit of executive discretion in bringing laws into operation; and

(j) legislative amendments in relation to the "911" incident and the development of communications technology in recent years.

1.3 Methodology

1.3.1 This research adopts a desk research method, which involves Internet research, literature review, documentation analysis and correspondence with relevant authorities.

Chapter 2 - The United Kingdom

2.1 Background

2.1.1 In the UK, interception of communications conducted by the government has been a long established and publicly known practice.[1] Before 1985, there was no overall statutory framework governing the practice which was regulated in part by provisions in various ordinances, and thus its legal basis was obscure. The power was vested in the Secretary of State to authorize by warrant the interception of postal and telegraphic communications, implying that the process was subject to executive control instead of statutory regulation.[2]

2.1.2 Between 1957 and 1981, the UK government had three official reports made available to the public, namely the 1957 Birkett Report, the 1980 White Paper and the 1981 Diplock Report.[3] These reports provided a review of the procedures, safeguards and monitoring arrangements relating to interception of communications, but none of them recommended a single legal framework to cover all interception matters.

---

1 Home Office (1999) p. 3 and European Court of Human Rights (1984) p. 7. The first public reference to a warrant of the Secretary of State authorizing the opening of letters is the Proclamation of 25 May 1663. In 1937, it was decided, as a matter of policy, that interception of telephone conversations had to be authorized by a warrant signed by the Secretary of State.

2 European Court of Human Rights (1984) pp. 5-10.

3 The Birkett Report was prepared by the Committee of Privy Councillors under the chairmanship of Lord Birkett. It mainly provided principles governing the issue of warrants to the Security Service. The 1980 White Paper aimed at bringing up to date the account of interception matters described in the Birkett Report, and confirmed the executive authority to issue interception warrants. Prepared by Lord Diplock who was a Lord of Appeal in Ordinary, the Diplock Report acted as an ongoing independent check on whether interception was carried out in accordance with the established purposes and procedures. See European Court of Human Rights (1984) p. 6 and Home Office (1999) pp. 3-4.

2.1.3 It was not until 1985 did the government indicate in a White Paper its intention to introduce legislation on interception of communications. The need for legislation was prompted by the European Court of Human Rights judgment on the Malone v. UK case in 1984.[4] In that case, the Court ruled that although the domestic law had detailed procedures governing interception of communications, it did not indicate clearly what elements of the power to intercept were incorporated in legal rules, and what elements remained within the discretion of the executive branch.[5] The Court further ruled that police interception of an individual's communications was a violation of Article 8 of the European Convention on Human Rights (ECHR).[6]

2.1.4 Following the issuance of the 1985 White Paper, the Interception of Communications Act 1985 (IOCA) was enacted. IOCA placed interception of communications sent by post or through a public telecommunications system on a statutory basis for the first time.[7] It created an offence of unlawful interception of communications, enshrined in law the framework for the operation of a warrant system, and set out safeguards, monitoring, and complaint mechanisms.[8]

2.1.5 Since IOCA was enacted, there have been enormous changes in telecommunications technology and communications services, such as the mounting popularity of mobile phones and communications via the Internet, the expansion of non-public telecommunications networks, and the surge in the number of private companies offering parcel and document delivery services. These changes have given rise to new human rights concerns and gone beyond the regulatory scope of IOCA. As such, the UK government recognized the need for new legislation as portrayed in a consultation paper published in 1999.[9] A year later, IOCA was repealed and replaced by the Regulation of Investigatory Powers Act 2000 (RIPA), which has become the primary legislation regulating interception of communications in the UK.

---

4 Home Office (1999) p. 5.

5 European Court of Human Rights (1984) pp. 28-29.

6 Under Article 8 of ECHR, "*everyone has the right to respect for his private and family life, his home and his correspondence*", and :"*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 Convention is available at http://www.hrcr.org/docs/Eur_Convention/euroconv3.html.

7 Home Office (1999) p. 5.

8 Ibid.

9 Home Office (1999).

2.2 Legal framework

2.2.1 RIPA contains five parts where Part I and Part IV form the legal framework for interception of communications.[10] The main objectives of Part I are to define the offences of unlawful interception, set out the circumstances in which interception is lawful, establish a system for authorization and issue of warrants, make requirements for interception capability, and impose restrictions on use of intercepted materials. Part IV is mainly concerned with the scrutiny of investigatory powers, including the establishment of an independent judicial oversight and a tribunal as a means of redress for those who wish to complain about the use of the powers.

2.2.2 Like IOCA, RIPA makes it an offence for anyone to intentionally intercept, without lawful authority, a communication transmitted through a public postal service or a public telecommunications system in the UK. However, unlike IOCA, RIPA extends the regulation to private telecommunications which include mobile phones, pagers and electronic messages over the computer networks.

2.2.3 Under RIPA,[11] a person intercepts a communication in the course of its transmission when that person makes "*some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication*" through modifying or interfering with the transmission system or monitoring the transmission. RIPA defines communications as those that are "*in the process of transmission*" and/or "*being stored on the transmission system*".[12] As such, "*stored communications*" are also regulated by RIPA.

[10] RIPA does not solely concern interception of communications. It also regulates other investigatory powers, including intrusive surveillance on residential premises or private vehicles, covert surveillance in the course of specific operations, the use of covert human intelligence sources, and access to encrypted data. See Part II and Part III of RIPA.

[11] Section 2, RIPA.

[12] Section 2 (7), RIPA and Home Office (2002) pp. 5-6.

2.2.4 The enforcement of RIPA coincided with the implementation of the Human Rights Act 1998, which incorporated ECHR into the UK law.[13] RIPA is required to reflect the requirements of Article 8 of ECHR, and to implement the directive issued by the European Parliament and the Council of the European Union, which requires member states to safeguard the confidentiality of communications.[14]

2.3 Interception warrant system under the Regulation of Investigatory Powers Act 2000

2.3.1 RIPA establishes a system under which a warrant issued by the executive branch is required for lawful interception of a communication.

2.3.2 There are two types of interception warrants. The first type, known as "*normal warrants*", requires one to name or describe either a person as "*the interception subject*" or a single set of premises where the interception is to take place.[15] Intercepting agencies usually apply for this type of warrants. The other type of warrants, known as "*certificated warrants*", requires a certificate issued by the Secretary of State and is only applied to "*external communications*" sent or received outside the UK. This type of warrants is exempt from, among others, the requirements to specify a person or premises.[16]

2.3.3 Despite their differences in various aspects, both types of warrants are subject to largely the same regulatory regime.

---

13 Under the Human Rights Act 1998, UK citizens are able to assert their rights guaranteed under ECHR through the national courts without having to take their cases to the European Court of Human Rights. For further information, see http://www.lcd.gov.uk/hract/hramenu.htm.

14 Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector. Its article 5 (1) states that "*Member States shall ensure via national regulations the confidentiality of communications by means of a public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorized, in accordance with Article 14 (1).*" Article 14 (1) states that "*Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 5…when such restriction constitutes a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the telecommunications system…*".

15 Section 8 (1), (2) and (3), RIPA.

16 Section 8 (4) and (5), RIPA.

Issuing authority

2.3.4 Both normal and certificated warrants must be issued by the Secretary of State, usually the Home Secretary who is responsible for law and order in the UK. Even in an urgent case where a warrant can be signed by a senior official, the Secretary of State must have considered the application and given instructions to the official before the signing of that particular warrant.[17]

Application procedures

2.3.5 The application[18] for normal or certificated warrants can be made only by or on behalf of a limited number of high-level officials, including:[19]

(a) the heads of security and intelligence agencies, namely the Director-General of the Security Service (MI5); the Chief of the Secret Intelligence Service (MI6); the Director of Government Communications Headquarters (GCHQ); the Director-General of the National Criminal Intelligence Service (NCIS); and the Chief of Defence Intelligence Staff (DIS)[20]; and

(b) the heads of law enforcement agencies, namely the Commissioner of Police of the Metropolis[21]; the Chief Constable of the Police Service of Northern Ireland; the Chief Constable of any police force maintained under the Police (Scotland) Act 1967; and the Commissioners of Customs and Excise.

---

17 According to the Interception of Communications Code of Practice published by the Home Office, an urgent case is one in which interception authorization is required within 24 hours. See Home Office (2002) pp. 12, 19 and 20.

18 Each application is required to contain the following information: the person or the set of premises to which the application relates; a description of the communications to be intercepted, details of the communications service providers, and an assessment of the feasibility of the interception operation; an explanation of why the interception is considered necessary; a consideration of why the conduct to be authorized by the warrant is proportionate to what is sought to be achieved by that conduct; a consideration of any unusual degree of infringement of the privacy of individuals other than the interception subject; and an assurance that all materials intercepted will be safeguarded, as stipulated under RIPA. In addition, the application for a certificated warrant must be accompanied by a certificate, issued by the Secretary of State, which specifies the extent to which the materials intercepted will be examined. See Home Office (2002) pp. 10, 11, 16 and 17.

19 Section 6, RIPA.

20 MI5 is charged with the British internal security, and MI6 the British external security. GCHQ mainly provides signals intelligence in the fields of national security, military operations and law enforcement. NCIS provides intelligence on serious and organized crimes. DIS is part of the Ministry of Defence, which provides strategic defence intelligence about possible threats to the UK and its allies.

21 The Metropolitan Police Service is the largest police force operating in Greater London.

Grounds on which warrants are issued

2.3.6 Before issuing a normal or certificated warrant, the Secretary of State must ensure that the application meets the following requirements:[22]

(a) the warrant is "*necessary*" in that it is "*in the interests of national security*", or for the purpose of "*preventing or detecting serious crime*", "*safeguarding the economic well-being*" of the UK against threats from overseas or "*giving effect to the provisions of any international mutual assistance agreement*";

(b) the conduct authorized by the warrant is "*proportionate*" to what that conduct seeks to achieve; and

(c) the information sought could not reasonably be obtained by other means.

Duration, termination and renewal of warrants

2.3.7 All new warrants, whether normal or certificated, are usually valid for an initial period of three months. Where necessary on the same grounds as a warrant has initially been granted, the warrant may be extended. Warrants renewed on serious crime grounds are valid for a further period of three months. Those renewed on national security or national economic well-being grounds are valid for a further period of six months. Warrants authorized for urgent cases are valid for five working days unless renewed by the Secretary of State. Warrants can be cancelled early if they are considered no longer proportionate to and necessary on the grounds that they were issued.

[22] Section 5, RIPA. Civil liberty organizations have criticized that some of the statutory grounds are vague and not defined, and too much discretion is conferred upon the Secretary of State. In response to these criticisms, the Home Office states that most of the wording of the grounds, such as "*necessary*", "*in the interests of national security*", and "*economic well-being*", come from Article 8 of ECHR (see footnote 6). In addition, the Secretary of State will not issue a warrant for the purpose of safeguarding the economic well-being of the UK, unless that purpose is proved to be directly linked with national security. See House of Commons Library (2000) pp. 28-29, and Home Office (2002) p. 8 and p. 11.

Lawful interception without a warrant

2.3.8 RIPA sets out a number of circumstances in which interception can lawfully take place without a warrant. Such circumstances include:[23]

(a) there are reasonable grounds to believe that both the sender and the intended recipient of a communication have consented to the interception;

(b) either the sender or intended recipient of a communication has consented to the interception, which has been authorized as surveillance rather than by an interception warrant.[24] Surveillance may arise, for example, when a kidnapper is telephoning relatives of a hostage, and the police wish to record the call in order to identify or trace the kidnapper; and

(c) interception is conducted in relation to the provision or operation of services. For example, the postal provider needs to open a postal item to determine the address of the sender because the recipient's address is unknown.

2.3.9 The Secretary of State can make regulations to permit certain kinds of interception in the course of lawful business practice, in hospitals, and under prison rules and international mutual assistance agreements. [25]

Internal safeguard measures

2.3.10 RIPA requires intercepting agencies to make internal safeguards on all materials intercepted under a normal or certificated warrant.[26]

23 Section 3, RIPA.

24 Section 48 (2) and (4), RIPA. Surveillance is a system of participant monitoring, which covers directed and intrusive surveillance and covert human intelligence techniques that may be used by the police or the intelligence services.

25 Section 4, RIPA.

26 Sections 15 and 16, RIPA and Home Office (2002) pp. 22-27.

Restrictions on use of intercepted materials

2.3.11 The disclosure, copying and retention of intercepted materials must be limited to the minimum necessary for the authorized purposes. These purposes include facilitating the carrying out of functions by the Interception of Communications Commissioner, and securing the fairness of prosecutions. Extra safeguards are in place for materials intercepted from external communications under certificated warrants. The Secretary of State must ensure that intercepted materials are read, looked at or listened to by any person only to the extent that the materials are certified.

2.3.12 In addition, only persons on the distribution list of each intercepting agency can have access to intercepted materials or see any report about them. All such persons must be appropriately vetted.[27]

Intercepted materials excluded from legal proceedings

2.3.13 Intercepted materials are not admissible as evidence in legal proceedings. Nor is questioning, assertion or disclosure likely to reveal that an interception has been made permitted. The only exceptions are when a prosecutor needs to review all available materials to ensure that the prosecution is not proceeding unfairly, or when the prosecutor has consulted the trial Judge who is satisfied that the exceptional circumstances of the case make the disclosure "*essential in the interests of justice*".[28]

Monitoring by judiciary

2.3.14 While there is no judicial involvement in granting interception warrants, RIPA provides for the Interception of Communications Commissioner, who must hold or have held high judicial office, to oversee the use of interception powers.[29]

---

27 Home Office (2002) p. 24.

28 Sections 17 and 18, RIPA, Home Office (2002) pp. 25-27, and the legal guidelines on telephone intercepts published by the Crown Prosecution Service at http://www.cps.gov.uk/legal/section20/chapter_e.html.

29 The Commissioner is appointed by the Prime Minister for a three-year period with the possibility of re-appointment. The current Commissioner, who was re-appointed in 2003, is a retired High Court Judge. See Interception of Communications Commissioner, 10 Downing Street press notice, 28 March 2003, http://www.pm.gov.uk/output/Page3375.asp.

The Interception of Communications Commissioner

2.3.15 The Commissioner is responsible for reviewing the Secretary of State's role in interception warrantry, the operation of the regime for acquiring communications data and the adequacy of the arrangements for ensuring the product of interception is properly handled.[30] RIPA does not specify how these functions should be discharged. The current Commissioner discharges his functions by reviewing the warrant applications made by the intercepting agencies to the Secretary of State. The Commissioner regularly visits relevant public authorities, especially law enforcement agencies, to selectively examine interception warrants with the officers responsible for the relevant investigations.[31]

2.3.16 All those who are involved in requesting, authorizing or carrying out interception must provide the Commissioner with any documents or information the Commissioner needs to carry out his statutory functions.[32] The Commissioner can at any time report to the Prime Minister as he thinks fit.

2.3.17 The Commissioner is required to submit an annual report to the Prime Minister. The report is laid before Parliament and then made available to the public. It includes a review of the interception processes and a summary of the value of the interceptions and, in a confidential annex which is not published, accounts of the operational successes achieved as a result of the interception warrants the Commissioner has reviewed.[33]

30 Section 57, RIPA and House of Lords (2000).

31 In 2003, the public authorities visited by the Commissioner are MI5, MI6, GCHQ, NCIS, the Special Branch of the Metropolitan Police, Strathclyde Police, the Police Service for Northern Ireland, Customs and Excise, the Foreign and Commonwealth Office, the Home Office, the Scottish Executive (the government of Scotland) and the Ministry of Defence. The Commissioner also talked to the Home Secretary, the Secretary of State for Northern Ireland, the Secretary of State for Defence and the First Minister for Scotland (the head of the government of Scotland). See Report of the Interception of Communications Commissioner for 2003 (2004) p.2.

32 Section 58, RIPA.

33 If the Prime Minister considers that the publication of any matter in an annual report would be contrary to the public interest or prejudicial to national security, the prevention or detection of serious crimes, the economic well-being of the UK or the continued discharge of the functions of any public authority overseen by the Commissioner, the Prime Minister can exclude that matter from the report laid before Parliament.

2.3.18 In the 2003 annual report, the Commissioner expressed his satisfaction that the warrants "*fully meet the requirements of RIPA, that proper procedures have been followed, and that the relevant safeguards and codes of practice have been followed*".[34] The Commissioner made the same comment in his annual reports for both 2001 and 2002 as well.[35]

Monitoring by legislature

2.3.19 The expenditure, administration and policies relating to interception of communications conducted by MI5, MI6 and GCHQ are monitored by a parliamentary committee known as the Intelligence and Security Committee (ISC).

The Intelligence and Security Committee

2.3.20 Established under the Intelligence Services Act 1994 (ISA), ISC comprises nine members selected from both the House of Commons and the House of Lords.[36] It submits an annual report to the Prime Minister, who lays the report subject to any deletion on security grounds before Parliament. It also provides ad hoc reports to the Prime Minister from time to time.

2.3.21 The disclosure of information by intelligence and security agencies to ISC is restricted by ISA. The directors of those agencies can share sensitive information with ISC. However, they may withhold information, with the agreement of the Home Secretary, for security purposes.

---

34 Report of the Interception of Communications Commissioner for 2003 (2004) p. 2.

35 Report of the Interception of Communications Commissioner for 2001 (2002) p. 2, and Report of the Interception of Communications Commissioner for 2002 (2003) p. 2.

36 The members of ISC are appointed by the Prime Minister in consultation with the Leader of the Opposition. Current Ministers are not allowed to be ISC members. At present, six ISC members, including the Chair, come from the Labour Party. ISC is supported by a clerk and a secretariat based in the Cabinet Office. In 1998, the UK government accepted ISC's proposal that an Investigator should be appointed to assist the Committee in fulfilling its remit. It was agreed that the Investigator would have access to the security and intelligence agencies, subject to the same considerations of sensitivity as applicable to ISC itself. A number of investigations have since been undertaken by the Investigator, and the findings are reflected in ISC's annual reports.

Monitoring by public

2.3.22 Any member of the public who is aggrieved by any interception activities conducted by or on behalf of the intercepting agencies can complain to the Investigatory Powers Tribunal (the Tribunal) established under RIPA.[37]

The Investigatory Powers Tribunal

2.3.23 The Tribunal is made up of eight senior members of the legal profession and the judiciary. All members are appointed by the Queen by Letters Patent.[38] The President of the Tribunal is currently a Lord Justice of Appeal.[39]

2.3.24 The Tribunal has power to hear and determine complaints and proceedings, award compensation, quash or cancel any warrant or authorization, and require the destruction of intercepted materials. It can also determine its own procedure regarding any proceeding, complaint or reference. Complaints are handled in confidence.[40] When determining a complaint, the Tribunal applies the same principles as those applied by a court on an application for judicial review. The complainant has no right of access to the relevant files. Unless the Secretary of State orders otherwise, the decision by the Tribunal is not subject to appeal or liable to be questioned in any court.

Number of complaints handled by the Investigatory Powers Tribunal

2.3.25 The Tribunal received 102 complaints from the day of its formation on 2 October 2000 to end 2001, and received 130 and 109 new complaints during 2002 and 2003 respectively. On no occasion did the Tribunal conclude that there was a contravention of RIPA or the Human Rights Act 1998.[41] Its predecessor, the Interception of Communications Tribunal, also did not uphold a single complaint in its 13 years of operation.

---

37 Sections 65 to 69, RIPA. This unified Tribunal is the replacement of the tribunals established under IOCA, the Security Service 1989, the Intelligence Services Act 1994 and the Police Act 1997.

38 RIPA does not specify the number and length of term of the members in the Tribunal. When the Tribunal was set up in 2000, its members were appointed for a term of five years.

39 Investigatory Powers Tribunal, http://www.homeoffice.gov.uk/inside/pubapps/ipt.html.

40 Investigatory Powers Tribunal: Regulation of Investigatory Powers Act 2000, www.dumgal.gov.uk/services/depts/tradstds/TribunalInfo.pdf.

41 See reports of the Interception of Communications Commissioner for 2001, 2002 and 2003.

Limit of executive discretion in bringing laws into operation

2.3.26 In the UK, the Prime Minister and Ministers do not have discretion in determining when to bring an act into operation after it has been enacted by Parliament. In principle, an act comes into operation immediately on Royal Assent. In reality, the act may empower a Minister to bring it into force by Order, and not necessarily all at once. This means that portions of an act may begin to operate later or may never come into operation before it is repealed. In the case of RIPA, not all of its sections were brought into operation when it was enacted in 2000. This was not because RIPA had operational difficulties, but because some of its sections took longer time to prepare for implementation.

2.4 Legislative amendments in relation to the "911" incident and the development of communications technology

2.4.1 In recent years, the UK government has introduced a number of legislative measures relating to interception of communications. Some of them focus on enhancing the implementation of RIPA to better cope with the development in communications technology and services, while others aim at strengthening the government's investigatory powers in the light of the "911" incident.

Interception of Communications Code of Practice

2.4.2 As required by RIPA, the Home Office published in July 2002 the Interception of Communications Code of Practice under the Regulation of Investigatory Powers (Interception of Communications: Code of Practice) Order 2002. The draft of the Code had gone through a public consultation process before it was approved by both Houses of Parliament.[42]

[42] Section 71 (4), RIPA and Draft Regulation of Investigatory Powers (Interception of Communications: Code of Practice) Order 2002, Minutes of House of Commons Third Standing Committee on Delegation Legislation, 21 May 2002, http://www.publiscations.parliament.uk.

2.4.3 The Code sets out in detail the procedures to be followed by public authorities that are empowered to apply for interception warrants and to conduct interception lawfully without a warrant in specific circumstances. It also provides guidelines on giving effect to warrants and the disclosure, copying, retention and other safeguards necessary for intercepted materials. Under RIPA, any person exercising interception powers and duties must have regard to the provisions in the Code, and the Code is admissible as evidence in criminal and civil proceedings. However, a person's failure to comply with the Code does not in itself render that person liable to criminal or civil proceedings.

Interception capability of communications service providers

2.4.4 In 2002, the Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002[43] was enacted in pursuance of section 12 of RIPA under which the Home Secretary can give notice to a communications service provider (CSP), such as a postal, telecommunications or internet company, requiring it to maintain an interception capability.[44] CSPs are obliged to provide assistance in giving effect to an interception warrant. Such obligations include providing intercepted materials to the relevant agencies, maintaining security and confidentiality, and facilitating the execution of the functions of the Interception of Communications Commissioner. Regarding the interception costs resulting from such obligations, the UK government is obliged under agreements with all CSPs providing interception to pay a "*fair contribution*" to cover the costs.[45]

Establishment of the Technical Advisory Board

2.4.5 If a CSP is served a notice to provide interception assistance and considers the technical or financial consequences of complying with the notice to be unreasonable, the CSP can refer it to the Technical Advisory Board (TAB).[46] Comprising representatives from the UK government and the communications industry, TAB advises the Home Secretary on the reasonableness of any notice referred to it. After considering a report from TAB, the Secretary of State may either withdraw the notice or give further notice confirming its effect, with or without modifications.[47]

---

43 Statutory Instrument 2002 No. 1931, http://www.hmso.gov.uk/si/si2002/20021931.htm.

44 Delegated Legislation Committee Debates. Tenth Standing Committee on Delegated Legislation. Draft Regulation of Investigatory Powers (Maintenance of Interception Capability). House of Commons. 18 June 2002.

45 Section 14, RIPA

46 Statutory Instrument 2001 No. 3734. TAB was established in November 2001 under the Regulation of Investigatory Powers (Technical Advisory Board) Order 2001.

47 Delegated Legislation Committee Debates. Tenth Standing Committee on Delegated Legislation. Draft Regulation of Investigatory Powers (Maintenance of Interception Capability). House of Commons. 18 June 2002.

The Anti-terrorism, Crime and Security Act 2001

2.4.6 The Anti-terrorism, Crime and Security Act 2001 was enacted in December 2001 as part of the emergency counter-terrorism legislation. It aims at ensuring that the UK government has the necessary powers to counter any threat to the UK. Under Part 11 of the Act, the Home Secretary can issue a code of practice relating to the retention of communications data by CSPs.

2.4.7 Communications data is information held by CSPs relating to the communications made by their customers, which includes itemized billing, routing information and subscriber details, but not the content of any communication. Under the Act, CSPs are permitted to retain such data beyond the period required for their own business purposes, so that it can be accessed by law enforcement and security agencies on national security and crime prevention grounds under RIPA.

Chapter 3 - The United States

3.1 Background

3.1.1 Interception of communications by the government has a long history in the US. Law enforcement agencies have practised wiretapping since the invention of telegraph communication in 1844, and tapping of telephones since the early 1890s.[48]

3.1.2 State statutes forbidding unlawful interception of communications were enacted as early as 1862.[49] However, federal laws had been silent on the matter for decades. In 1928, the Supreme Court ruled in the case of Olmstead v. United States that interception of telephone conversations by federal agents using a wiretap did not constitute a search or seizure under the meaning of the Fourth Amendment to the Constitution.[50] The main argument was that in the Fourth Amendment, protection against unreasonable searches and seizures applied only to persons or physical things, not intangibles such as telephone conversations.

3.1.3 The year 1934 witnessed the enactment of the Federal Communications Act of 1934, which was the first federal law prohibiting interception and divulgence of telephone conversations without the consent of the sender. The Act also limited the use of intercepted materials as admissible evidence in legal proceedings. However, the effectiveness of the Act was quickly eroded by executive powers. In the following 30 years, the federal investigative authorities continued to intercept communications at their discretion, mainly against suspected foreign agents under the President's constitutional authority to protect national security.[51]

3.1.4 In the 1960s, the Supreme Court sought to protect individuals from unreasonable searches and seizures by circumscribing prosecution based on interception of communications. In the landmark case of Katz v. United States in 1967, the Court established the doctrine of reasonable expectation of privacy by ruling that interception without a warrant is against the Fourth Amendment. This ruling overturned the 1928 Olmstead judgment, and the Court ruled that interception of communications was permissible only if it was constitutionally acceptable.

---

48 Boucher, Cotler and Larson (2001) p. 3, Edwardson (1999) p. 1 and The New Encyclopaedia Britannica (1994) p. 437.

49 The New Encyclopaedia Britannica (1994) p. 437.

50 The Fourth Amendment to the Constitution states that "*the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*"

51 Boucher, Cotler and Larson (2001) p. 3 and p. 14, and The New Encyclopaedia Britannica (1994) p. 437.

3.1.5 In 1968, Congress enacted Title III of the Omnibus Safe Streets and Crime Control Act 1968 (commonly referred to as Title III), creating at the federal level the first specific legal framework for interception of communications. Since then, Congress has revised and updated interception laws on a number of occasions. The Foreign Intelligence Surveillance Act (FISA), the Electronic Communications Privacy Act (ECPA), and the Communications Assistance for Law Enforcement Act (CALEA) were enacted in 1978, 1986 and 1994 respectively. The latest significant revision of interception laws was the enactment of the Uniting and Strengthening of America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (the PATRIOT Act) one and a half months after the "911" incident in 2001.

3.2 Legal framework

3.2.1 The federal legal framework for interception of communications has three main components:

(a) Title III in 18 U.S.C.§§ 2510-2522 and its amendments made by ECPA;

(b) FISA in 50 U.S.C.§§ 1801-1811; and

(c) the Pen Registers and Trap and Trace Devices chapter of Title 18 (the Pen/Trap statute) in 18 U.S.C.§§ 3121-3127.

Title III of the Omnibus Safe Streets and Crime Control Act 1968

3.2.2 Title III has been the most important federal statute regulating the real-time "*collection of actual contents*" of wire and oral communications for law enforcement purposes.[52] "*Contents*" here include "*any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication*".[53] The statute was amended by ECPA in 1986 to include interception of electronic communications.[54]

3.2.3 Under Title III, "*intercept*" means "*the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device*". According to the Department of Justice, the meaning of "*intercept*" is "*restricted to acquisitions of communications contemporaneous with their transmissions*", and does not cover the acquisition of stored wire or electronic communications.[55] Therefore, Title III is applicable only to real-time interception of communications, but not to the acquisition of stored communications.

The Foreign Intelligence Surveillance Act of 1978

3.2.4 FISA provides for interception of communications of foreign powers[56] or their agents within the US for the purpose of obtaining foreign intelligence information. This information is defined in terms of the US national security, including defence against actual or potential attack, sabotage, international terrorism, and clandestine intelligence activities, among others.

---

52 Department of Justice (2002) pp. 76-77. Under Title III, oral communication means spoken words "*uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation*". Wire communication means "*a transfer containing the human voice at any point between and including the point of origin and point of reception*", and must be sent in whole or in part "*by the aid of wire, cable or other like connection*". In general, telephone conversations are wire communications. See Section 2510, Title III and Department of Justice (2002) p. 81.

53 Section 2510 (8), Title III.

54 Under Title III, electronic communication means "*any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system*". Most Internet communications, including e-mails, are electronic communications. Electronic communication does not include the following: any wire or oral communication; any communication made through a tone-only paging device; any communication from a tracking device; or electronic funds transfer information stored by a financial institution in a communication system used for the electronic storage and transfer of funds.

55 Department of Justice (2002) pp. 82-83.

56 Under section 1801(a) of FISA, "foreign power" includes a foreign government or its component; a faction of a foreign nation which is not substantially composed of US persons; an entity that is or is to be directed and controlled by a foreign government; a group engaged in international terrorism; and a foreign-based political organization which is not substantially composed of US persons.

3.2.5 Similar to Title III, FISA regulates interception of the actual "*contents*" of communications.[57] Unlike Title III, FISA's target of surveillance must be a foreign power or its agent in the US, or the facilities under surveillance are being used or are about to be used by a foreign power or its agents. The targeted communications need not relate to any crime, although the information to be sought may yield evidence for criminal prosecution. Nonetheless, a significant purpose of the surveillance must be to obtain foreign intelligence information instead of carrying out law enforcement.

The Pen Registers and Trap and Trace Devices chapter of Title 18

3.2.6 Unlike Title III or FISA, the Pen/Trap statute regulates the real-time "*collection of addressing and other non-content information*" of wire and electronic communications, such as the phone numbers dialed for outgoing calls and those of incoming calls.[58]

3.2.7 According to the Department of Justice, both "*Pen register*" and "*Trap and trace device*" are so broadly defined that intercepting devices can be any physical tool or software programme, or be installed into a wide variety of communications technologies, including cellular telephones, Internet user accounts or e-mail accounts. It can also record or decode almost all non-content information in a communication.[59]

3.3 Court order system under Title III of the Omnibus Safe Streets and Crime Control Act 1968

3.3.1 Under Title III, federal investigative or law enforcement officers are permitted to intercept communications pursuant to court orders.

---

[57] Section 1801 (n), FISA. The definition of "*contents*" under FISA is basically the same as that under Title III.

[58] Ibid. Under the Pen/Trap statute, "*pen register*" means "*a device or process which records or decodes dialing, routing, addressing or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted*", provided that such information does "*not include the contents of any communication*". The term also does not include devices or processes used for billing or cost accounting. "*Trap and trace device*" means "*a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing and signaling information reasonably likely to identify the source of a wire or electronic communication*", and such information does "*not include the contents of any communication*".

[59] Department of Justice (2002) pp. 104-105.

Issuing authority

3.3.2 A Title III court order must be issued by a Judge of a US District Court or a US Court of Appeals.[60]

Application procedures

3.3.3 Before being approved by a Judge, each application must have the authorization by one of the following high-level officials of the Department of Justice:[61]

(a) the Attorney General;

(b) the Deputy Attorney General;

(c) the Associate Attorney General; or

(d) any Assistant Attorney General, any acting Assistant Attorney General or any specially designated Deputy Assistant Attorney General.

3.3.4 Each application must be made in writing upon oath or affirmation to a Judge.[62] If necessary, the applicant may be required to furnish the Judge additional testimony or documentary evidence in support of the application.

Grounds on which court orders are issued

3.3.5 A court order can be issued only for investigating serious crimes listed in Title III. Such crimes include murder, kidnapping, robbery, extortion, bribery, child molestation, narcotics offences, crimes against national security, and any offence punishable by death or by imprisonment for more than one year, among others.[63]

---

60 Section 2510 (9). Title III.

61 Section 2516, Title III.

62 Section 2518, Title III. Each application must include the following information: (a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application; (b) the facts and circumstances relied upon by the applicant to justify his or her belief that an order must be issued. Such facts include details of the offence that has been, is being or is about to be committed; a description of the nature and location of the facilities or the place where the communication is to be intercepted and the type of communications to be intercepted; and the identity of the person, if known, committing the offence and whose communications are to be intercepted; (c) whether or not other investigative procedures have been tried and failed, or why they are reasonably determined to be unlikely to succeed if tried or to be too dangerous; (d) the period for which the interception is required to be maintained; and (e) particulars of all previous applications.

63 Section 2516 (1) (a) to (r), Title III.

3.3.6 Moreover, the application must demonstrate "*probable cause*" for the Court to believe that:[64]

(a) an individual is committing, has committed, or is about to commit a particular offence listed in Title III;

(b) particular communications concerning that offence will be obtained through such interception; and

(c) the facilities or the place where the wire, oral or electronic communications are to be intercepted are being used, or are about to be used, or are commonly used by that individual.

3.3.7 The application must also show that the interception will be conducted in such a way as to "*minimize the interception of communications not otherwise subject to interception*",[65] such as unrelated, irrelevant and non-criminal communications of the subjects or others not named in the application.[66]

3.3.8 Under Title III,[67] intercepting agencies can apply for "*roving taps*", meaning that they can get a court order that does not name a specific telephone line or email account, but allows them to tap any phone line, cell phone or Internet account that a suspect uses. Roving taps are granted if there is probable cause to believe that the interception subject is attempting to thwart interception from a specified facility, e.g. switching telephones to evade interception.

3.3.9 Upon request of the applicant, the court order may require the third parties concerned, such as CSPs and the landlord, to provide information, facilities and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services. The order may also require the third parties concerned to comply with the interception capability requirements under CALEA.[68] Under CALEA, these third parties will be reasonably compensated for expenses incurred in providing such facilities and technical assistance.

---

64 Section 2518 (3), Title III.

65 Kerr (2000) p.2, and Section 2518 (5), Title III.

66 Ibid.

67 Section 2518 (11) (b), Title III. Roving taps are relatively rare. In 2003, only six roving taps were approved in criminal cases under Title III. Of those, one was for a federal narcotics investigation; and the other five were at the state level: three applications in racketeering investigation, one application in a narcotics investigation, and one application in a murder investigation. See 2003 Wiretap Report (2004).

68 Ibid.

Duration, termination and renewal of court orders

3.3.10 The court order must "*minimize the interception of communications*", implying that the interception must not continue for "*any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than 30 days*".[69] Renewals of an order may be granted to extend the order, but a renewal cannot be longer than 30 days and must terminate when the authorized objectives are met.

Lawful interception without a court order

3.3.11 Title III provides that before obtaining a court order, a law enforcement official designated by the Attorney General, the Deputy Attorney General or the Associate Attorney General can initiate interception of communications in an emergency that involves:[70]

(a) immediate danger of death or serious injury to any person;

(b) conspiratorial activities threatening national security; or

(c) conspiratorial activities characteristic of organized crimes.

3.3.12 Nevertheless, the application for a court order must be made within 48 hours after the interception has occurred or begins to occur. If the application is not made or is denied, the interception must terminate immediately and will be treated as unlawful.[71]

69 Section 2518 (5), Title III.

70 Section 2518 (7) (a), Title III, and Schott (2003).

71 Section 2518 (7) (b), Title III. The Court has made clear that there are places, such as prison cells, patrol cars, interrogation rooms, where a person does not have a reasonable expectation of privacy. Therefore, no interception warrant is required to surreptitiously record conversations in such places, even when no one has consented to the recording. Under the Fourth Amendment, government searches which intrude into a person's reasonable expectation of privacy are prohibited. See Schott (2003).

Internal safeguard measures

Minimization of interception

3.3.13 To restrict the invasion of privacy, Title III requires the implementation of the minimization procedure. Typically, law enforcement officers are regarded as satisfying minimization obligations by turning off the interception equipment when contents outside the scope of the court order are heard, and turning the equipment back on periodically to determine if contents within the scope of the order are occurring.[72]

Recording of intercepted communications

3.3.14 Intercepted communications must be recorded on tape or other comparable devices, so as to protect the recording from editing or other alternations. Immediately upon the expiration of the interception period, these recordings must be made available to the Judge issuing the order and sealed under his or her directions. They must not be destroyed except upon an order of the issuing or denying Judge, and must be kept for 10 years.[73]

Protection of rights of people under surveillance

3.3.15 Within a reasonable time but not later than 90 days after the termination of the court order, the issuing Judge is obligated to ensure that the subject of the court order, and other parties as are deemed in the interest of justice, are furnished with an inventory, which includes notice of the dates during which the interception activities were carried out and whether the communications were intercepted. Upon application, the Judge can make portions of the intercepted materials, interception applications and court orders available to the affected person(s) for inspection.[74]

Submission of periodic reports

3.3.16 The Judge who issued the interception order usually requires the intercepting agency to submit periodic reports, typically every seven to 10 days, showing the progress of the interception operation.[75]

---

72 IIT Research Institute (2000) pp. 3-1 to 3-2.
73 Section 2518 (8) (a) and (b), Title III.
74 Section 2518 (8) (d), Title III.
75 Kerr (2000) p. 2.

Admissibility of evidence

3.3.17 Intercepted materials are admissible as evidence in court, but each relevant party must be furnished with a copy of the interception order and its application not less than 10 days before the trial. This 10-day period may be waived by the Judge if he or she finds that the relevant parties will not be prejudiced by the delay in receiving such information.[76]

Monitoring by judiciary

3.3.18 Within 30 days after the expiration (or the denial) of a court order (or its renewal), the issuing or denying Judge must report to the Administrative Office of the US Courts (the Administrative Office).[77] The report must include:[78]

(a) the identity of the official applying for the order and the person authorizing the application;

(b) the offence under investigation;

(c) the type of interception devices and the general location of those devices; and

(d) the duration of interception authorized by the order.

[76] Sections 2515 and 2518 (9), Title III.

[77] The Administrative Office was created by law (28 U.S.C. 601) in 1939. Its Director and Deputy Director are appointed by the Chief Justice of the US after consultation with the Judicial Conference of the US. It is charged with the non-judicial, administrative business of the Court, see http://www.uscourts.gov/contact.html.

[78] Section 2519 (1), Title III.

3.3.19 In January of each year, prosecutors who applied for court orders during the previous year must also report to the Administrative Office. The report must include:[79]

(a) items (a) to (d) listed in the above paragraph;

(b) the nature and frequency of incriminating and non-incriminating materials intercepted;

(c) the number of persons whose communications were intercepted;

(d) the number of orders in which encryption was encountered, and whether such encryption prevented law enforcement officers from obtaining the plain text of communications intercepted;

(e) the nature, amount and cost of manpower and other resources used in the interceptions; and

(f) the number of arrests, trials and convictions resulting from the interceptions.

Monitoring by legislature

3.3.20 Aside from judicial monitoring, Congress can exercise ongoing oversight over interception of communications in a number of ways.

Parliamentary committees

3.3.21 The Committee on the Judiciary and Intelligence can hold hearings, and submit written questions to be addressed by investigative or law enforcement agencies. Interception activities may also be monitored by both the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence. The two Committees are responsible for ensuring that intelligence resources are not misused and intelligence activities are conducted lawfully.[80]

[79] Section 2519 (2), Title III.

[80] See the websites of the two Committees at http://intelligence.house.gov/AboutTheCommittee.aspx and http://intelligence.senate.gov/juris.htm.

Report to Congress

3.3.22 In April of each year, the Director of the Administrative Office is required to report to Congress the number of interception applications and the number of court orders and extensions granted or denied during the preceding year; as well as an analysis of these data.[81]

Monitoring by public

3.3.23 Any person who is a party to an intercepted communication or a party against whom an interception is directed can in any legal proceeding apply for the suppression of the contents of any intercepted communication or any evidence derived from it. The grounds on which such applications can be made include: the communication is unlawfully intercepted; the court order approving the interception is insufficient; and the interception is not made in conformity with the court order.[82]

3.4 Court order system under the Foreign Intelligence Surveillance Act of 1978

3.4.1 Under FISA, the target of surveillance must be a foreign power or an agent of a foreign power in the US, and the facilities under surveillance are being used or are about to be used by a foreign power or its agents. If the interception involves the acquisition of communications of any US person within the US, it must be conducted with a court order.[83] The requirements for obtaining a court order are less restrictive than those outlined in Title III.

[81] Section 2519 (3), Title III.

[82] Section 2518 (10) (a), Title III.

[83] Under the Executive Order 12333, the President can authorize to intercept, without a court order, foreign powers and their agents for the purpose of acquiring intelligence information unrelated to the activities of US persons.

Issuing authority

3.4.2 A FISA order must be issued by a special court known as the FISA court. The court comprises 11 District Court Judges appointed by the Chief Justice of the Supreme Court from seven of the 11 US judicial circuits. The FISA court has sole jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the US. A Judge of the FISA court cannot hear the same application which has been denied previously by another Judge.[84]

Application procedures

3.4.3 Each application must be made by a federal officer in writing upon oath or affirmation to the issuing Judge, and must be authorized by the Attorney General.[85]

3.4.4 The application must contain a list of information similar to those in a Title III application. In addition, FISA requires the application to include a certification that "*a significant purpose of the surveillance is to obtain foreign intelligence information*".[86] The certification must be made by the Assistant to the President for National Security Affairs, or an executive branch official designated by the President from among those executive officers who are appointed by the President with the advice and consent of the Senate.

Grounds on which court orders are issued

3.4.5 Normally, the Judge grants an order if:[87]

(a) the President has authorized the Attorney General to approve the application;

(b) the application has been made by a federal officer and approved by the Attorney General;

---

84 Section 1803, FISA. If any Judge denies an application for a court order, he or she must provide for the record a written statement of the reasons for the decision, and the record is sent to the Court of Review for consideration. The Court of Review comprises three Judges, who are designated by the Chief Justice from the US District Courts or Courts of Appeals. It has jurisdiction to review the denial of application for court orders. If the Court of Review determines that the application is properly denied, it must provide for the record a written statement of the reasons for the decision, which can be further reviewed by the Supreme Court. Whilst up until 2003 the FISA court had never denied any application for an order, the court denied four applications in 2003, but the US government did not appeal against any of those decisions. See also the Attorney General's 2003 report submitted to the Administrative Office of the US Courts pursuant to FISA, 30 April 2004.

85 Section 1804 (a), FISA.

86 Section 1804 (a)(7)(B), FISA.

87 Section 1805 (a), FISA.

(c) there is probable cause to believe that the US person under electronic surveillance is a foreign power or its agent, and each facility or place at which the surveillance is directed is being used or is about to be used by a foreign power or its agents. An agent of a foreign power includes persons who knowingly engage in, or knowingly aid or abet individuals who engage in, clandestine intelligence activities, sabotage or international terrorism; and

(d) the intercepting agency has pledged to apply the minimization procedures of obtaining, retaining or disseminating intercepted information.

3.4.6 After the enactment of the PATRIOT Act, FISA is able to grant roving taps on the grounds as stipulated under Title III.

Duration, termination and renewal of court orders

3.4.7 In general, a FISA order runs for an initial period of up to 90 days. If targeted against a foreign power, the order is effective for up to one year. If targeted against an agent of a foreign power, the order is effective for up to 120 days. Extensions of an order may be granted on the same basis as an original order, upon an application for an extension and new findings made in the same manner as required for an original order.

Lawful interception without a court order

3.4.8 Under FISA, the President, through the Attorney General, can authorize electronic surveillance without a court order to acquire foreign intelligence information for up to one year, if the Attorney General certifies the following matters:

(a) the surveillance is solely directed at the acquisition of the contents of communications transmitted exclusively between or among foreign powers; or the acquisition of technical intelligence from properties or premises under the open and exclusive control of a foreign power;

(b) the surveillance will not cover communications to which a "*United States person*"[88] is a party; and

[88] Under section 1801(i) of FISA, "United States person" means a US citizen, an alien lawfully admitted for permanent residence, an unincorporated association whose members are substantially US citizens or lawful aliens, or a corporation which is incorporated in the US but does not include a corporation or an association which is a foreign power.

(c) the intercepting agency has pledged to implement the minimization procedures, and the Attorney General reports these minimization procedures to both the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least 30 days before the effective date of the procedures.[89]

Internal safeguard measures

3.4.9 Compared to the internal safeguard measures for Title III court orders, those for FISA court orders are less demanding.[90]

Restriction on disclosure and use of information

3.4.10 Unlike Title III, FISA does not require the target of surveillance to be notified that communications have been intercepted. Intercepted materials concerning any US person may be used and disclosed for lawful purposes by federal officers without the consent of the US person, provided that such use and disclosure comply with the minimization procedures.

Intercepted materials used in court

3.4.11 Subject to the approval of the Attorney General, intercepted materials are admissible as evidence in the court. Before using the materials, the government must notify the defendant who has the right to move to suppress such evidence if it was gathered unlawfully. However, the defendant is denied access to the FISA order or its application, if the Attorney General certifies that the release of these documents would harm national security.

Monitoring by judiciary

3.4.12 Similar to Title III, FISA requires the Attorney General to submit an annual report to the Administrative Office. Unlike in the case of Title III, the information disclosed about FISA interception is significantly limited. The Attorney General is required only to supply the overall number of applications for orders and extensions of orders approving electronic surveillance and physical search, and the respective number of such orders granted, modified and denied. All other information about FISA is classified.

---

89 If the Attorney General decides that immediate action is required, he or she must notify the two committees immediately of such minimization procedures and the reason for the decision.

90 Section 1806, FISA.

Monitoring by legislature

3.4.13 The Attorney General must submit the annual report to Congress as well. Moreover, the Attorney General is required twice every year to "*fully inform*" both the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence. The information provided must include a description of each criminal case in which information intercepted has been used for law enforcement purposes or has been authorized for use at trial.

3.5 Court order system under the Pen Registers and Trap and Trace Devices chapter of Title 18

3.5.1 The Pen/Trap court order system is less stringent than that under Title III or FISA.

Issuing authority

3.5.2 A Pen/Trap order must be issued by a US District Court (including a magistrate Judge of such a court) or a US Court of Appeals. In addition, the issuing court must have jurisdiction over the offence being investigated.[91]

Application procedures

3.5.3 An application can be made by any attorney for the federal government. No special authorization is required.[92]

Grounds on which court orders are issued

3.5.4 The court will approve the application so long as the applicant has certified that the information likely to be intercepted is relevant to an ongoing criminal investigation. The court has no obligation to conduct an independent judicial inquiry into the veracity of the facts contained in the application.

3.5.5 Similar to Title III orders, the Pen/Trap order can require third parties to provide interception assistance and comply with interception capability requirements under CALEA.

---

91 Sections 3122 and 3127 (2), the Pen/Trap statute.

92 Section 3122, the Pen/Trap statute. The application must include the identity of the applicant and the identity of the law enforcement agency conducting the investigation, and a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

Duration, termination and renewal of court orders

3.5.6 A Pen/Trap order is effective for not more than 60 days. The order may be extended, where necessary on the same grounds as the order has initially been granted. Each extension is for a period not exceeding 60 days.[93]

Lawful interception without a court order

3.5.7 Similar to Title III, the Pen/Trap statute allows an investigative or law enforcement officer designated by a high-level official of the Department of Justice to initiate interception without a court order in an emergency, as long as the application for an order is made within 48 hours after the interception starts. However, the definition of emergency under the Pen/Trap statute is simpler than that under Title III in that it only involves immediate danger of death or serious bodily injury to any person or conspiratorial activities characteristic of organized crimes, and does not involve conspiratorial activities threatening national security.

Internal safeguard measures

Restrictive use of intercepting technology

3.5.8 The Pen/Trap statute provides for a restriction on the use of the technology of the Pen/Trap devices by intercepting agencies. The recording or decoding of electronic or other impulses must be limited to the dialing, routing, addressing and signaling information, so that the contents of any communications are not included.[94]

Nondisclosure of existence of Pen/Trap devices

3.5.9 The court order must be sealed until ordered otherwise by the issuing court. The third parties who provide interception assistance to the applicant are also required not to disclose the existence of the Pen/Trap devices to any person, unless or until ordered otherwise by the court.[95]

Monitoring by judiciary

3.5.10 If a Pen/Trap device is used with any wiretap devices, such use must be reported to the Administrative Office. Apart from that, no report to the Administrative Office is required.

---

93 Section 3123 (c), the Pen/Trap statute.
94 Section 3121 (c), the Pen/Trap statute.
95 Section 3123 (d), the Pen/Trap statute.

Monitoring by legislature

3.5.11 The Attorney General is required to submit an annual report to Congress. The report must include:[96]

(a) the period of interceptions authorized by the order, and the number and duration of extensions of the order;

(b) the offence specified in the application and order, or extension of an order;

(c) the number of investigations involved;

(d) the number and nature of the facilities affected; and

(e) the identity, including district, of the applying investigative or law enforcement agency making the application and the person authorizing the order.

3.6 Limit of executive discretion in bringing laws into operation

3.6.1 The US's executive branch has discretion in deciding whether a law should be put into operation, but the power is subject to legislative constraint. Article 1, section 7 of the Constitution provides that "*every bill which shall have passed the House of Representatives and the Senate, shall, before it becomes a Law, be presented to the President of the United States.*" The President has 10 days to decide whether or not to sign a bill. If the President signs a bill, it becomes a law. If the President vetoes the bill, he must return it to Congress with a message indicating his reasons for disapproval. Congress may reconsider and modify the bill which is presented again to the President. If the President does not sign or return the bill within 10 days, the bill becomes a law automatically. Congress can override a Presidential veto by having a two-thirds majority vote in both Houses, and thus signing a bill into law despite the President's veto. Regarding the enactment of the interception laws, the executive branch had no difficulty in gaining the majority support of Congress and bringing the laws into operation, although it was criticized by civil liberty organizations for vastly expanding its power to invade the privacy of citizens.

[96] Section 3126, the Pen/Trap statute.

3.7 Legislative amendments in relation to the "911" incident and the development of communications technology

3.7.1 In the US, most of the recent legislative amendments made by Congress are related to the "911" incident, instead of the development of communications technology.

The Uniting and Strengthening of America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act

3.7.2 In response to the national security threats posed by terrorism after the "911" incident, Congress has passed a number of laws providing new tools to fight terrorism. One of the most controversial acts is the PATRIOT Act. The Act amends a number of existing statutes and contains new provisions covering a wide range of topics. Below are the major amendments made by the Act to federal interception laws giving federal officials greater authority to intercept communications for both law enforcement and foreign intelligence gathering purposes.[97]

Amendments to Title III

3.7.3 To the designated offence list in Title III, the PATRIOT Act adds cyber-crimes, such as computer frauds, and several terrorist crimes, such as chemical weapons offences, use of weapons of mass destruction, violent acts of terrorism transcending national borders, financial transactions with countries which support terrorists, material support of terrorists and material support of terrorist organizations.[98]

3.7.4 The PATRIOT Act introduces new provisions in Title III permitting investigative or law enforcement officers to intercept, without a court order, the communications of a trespasser within a "*protected computer*" system, such as computers used in interstate or foreign commerce or communications, or computers used by the federal government or financial institutions. The interception must be restricted to the trespasser's communications transmitted to, through or from the invaded computer.[99]

97 For details, see Doyle (2001) and (2002).
98 Sections 201 and 202, the PATRIOT Act.
99 Section 217, the PATRIOT Act.

3.7.5 The PATRIOT Act also introduces a new provision[100] in Title III permitting investigative or law enforcement officers to share contents of intercepted communications, including foreign intelligence, with other federal law enforcement, intelligence, protective, immigration, national defence or national security officials, in order to assist those officials in the performance of their official duties.

Amendments to FISA

3.7.6 Prior to the enactment of the PATRIOT Act, FISA provided that the interception application for a court order had to contain a certification by a designated official of the executive branch that "*the purpose*" for the surveillance was to obtain foreign intelligence information. The PATRIOT Act replaces "*the purpose*" with "*a significant purpose*".[101]

3.7.7 To encourage co-operation between law enforcement and foreign intelligence investigators, the PATRIOT Act provides that criminal investigative information that contains foreign intelligence or counterintelligence, including wiretap information, can be shared among intelligence officials.

Amendments to the Pen/Trap statute

3.7.8 Under the previous Pen/Trap statute, court orders authorizing Pen/Trap devices were mainly applied to telephone lines, although they had been applied by many courts to computer network communications. In addition, the use of Pen/Trap devices was restricted at one time to the judicial district in which the order was issued. According to the Department of Justice, this restriction wasted time and resources because law enforcement officers tracking a suspected criminal in multiple jurisdictions had to apply for a duplicative order in each jurisdiction. Under the PATRIOT Act, not only can Pen/Trap orders be used to capture source and addressee information for computer conversations such as emails, a court with jurisdiction over the crime under investigation can also issue an order to be executed anywhere within the US.[102]

[100] Section 203, the PATRIOT Act.
[101] Section 218, the PATRIOT Act.
[102] Section 216, the PATRIOT Act, Doyle (2002) pp. 5-6, and Mueller (2004) p.2.

Chapter 4 - Australia

4.1 Background

4.1.1 Before 1960, there had been no Commonwealth legislation prohibiting interception of communications in Australia. The Australian government's interception activities were conducted as an executive act. Starting from 1950, there were Prime Ministerial directions in place to govern the exercise of such executive power. These directions authorized interception only in relation to cases of espionage, sabotage and subversive activities.[103]

4.1.2 The first attempt to statutorily regulate interception of communications occurred in 1960 with the enactment of the Telephonic Communications (Interception) Act 1960. This Act made it a criminal offence to intercept telephonic communications except in two scenarios.[104] Telecommunications interception for law enforcement purposes was not permitted.

4.1.3 The 1960 Act was repealed and replaced by the Telecommunications (Interception) Act 1979 (the Interception Act), which created a "*Commonwealth monopoly of legal telephone interception*" and a structure for the power to be delegated to eligible authorities at the State level.[105] Under the Interception Act, law enforcement agencies, such as the Australian Federal Police and State police forces, were permitted for the first time to intercept telephone communications in certain circumstances.

4.1.4 Since 1979, the Interception Act has served as the primary legal framework for interception of telecommunications. Through amendments to the Interception Act, the offences that can be investigated under an interception warrant have multiplied, the number of agencies authorized to apply for interception warrants has increased, and the purposes for which intercepted materials can be used have been broadened.

---

103 Explanatory note on Telecommunications (Interception) Amendment Bill 1994, p.2.

104 In the first scenario, the interception was conducted by officers of the Postmaster-General's Department either for technical reasons or tracing unlawful calls such as nuisance calls. In the second scenario, it was under warrants issued either by the Attorney-General to the security service for national security purposes or by the Director-General of Security in emergencies and for a short term.

105 Explanatory note on Telecommunications (Interception) Amendment Bill 1994, p.3.

4.2 Legal framework

4.2.1 The statutory basis of the Interception Act derives from section 51 of the Commonwealth of Australia Constitution Act, which states that the Australian Parliament has power "*to make laws for the peace, order and good government of the Commonwealth*" with respect to "*postal, telegraph, telephonic, and other like services*".

4.2.2 The Interception Act focuses on two areas. The first focus is to "*protect the privacy of individuals who use the Australian telecommunications system by making it an offence to intercept communications passing over that system*".[106] Section 6(1) of the Interception Act defines "*interception*" as "*consisting of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication*". Under the Interception Act, stored communications are under protection from interception, as the term "*passing over*" includes the meaning of "*being stored temporarily*" on a telecommunications system. In recent years, the Australian government has been trying to introduce legislative amendments in the Australian Parliament to remove stored communications from the protection of the Interception Act.

4.2.3 The second focus of the Interception Act is to "*specify the circumstances in which it is lawful for interception to take place*".[107] The Act stipulates the purposes for which interception warrants may be obtained, who can apply for and issue these warrants, the form and content of warrant applications, the criteria that must be satisfied before warrants can be issued, the scope of warrants, and record keeping and reporting requirements.

4.3 Interception warrant system under the Telecommunications (Interception) Act 1979

4.3.1 There are two types of interception warrants, namely "*telecommunications service warrants*" and "*named person warrants*". The former is issued in relation to a particular identified telecommunications service, while the latter is issued in relation to any telecommunications service that is used or likely to be used by a named individual.

---

[106] Attorney-General's Department (2004) p.8. This focus is embedded in section 7(1) of the Interception Act, which states that "*a person shall not intercept; authorize, suffer or permit another person to intercept; or do any act or thing that will enable him or her or another person to intercept a communication passing over a telecommunications system*".

[107] Attorney-General's Department (2004) p.8, and section 7 (2) (b), the Interception Act.

Issuing authorities

4.3.2 Both types of warrants can be issued for either one of two purposes, namely national security and law enforcement.

The Attorney-General and Director-General of Security

4.3.3 National security warrants are normally issued by the Commonwealth Attorney-General (the Attorney-General), who is the minister responsible for police, legal affairs and the Australian Security Intelligence Organization (ASIO).[108] The Attorney-General is appointed by the Prime Minister who, by convention, is the leader of the party or coalition which has the most seats in the House of Representatives.

4.3.4 In limited circumstances, national security warrants that can be in force for not more than 48 hours may be issued by ASIO's Director-General of Security, who reports to the Attorney-General. Such circumstances include:[109]

(a) the Attorney-General has not, within the preceding three months, refused to issue a warrant requested by the Director-General of Security; and

(b) the Director-General of Security is satisfied that the facts of the case under investigation would justify the issue of a warrant by the Attorney-General, and that waiting for the Attorney-General's decision on the issue of a warrant will, or is likely to, seriously prejudice national security.

4.3.5 When issuing a warrant, the Director-General of Security must furnish to the Attorney-General a copy of the warrant and a statement of the grounds on which the warrant is issued. The warrant can be revoked by the Attorney-General at any time before it expires.[110]

[108] ASIO's functions are set out in the Australian Security Intelligence Organization Act 1979. Its main role is to gather information and produce intelligence, enabling it to warn the government about activities or situations that might endanger Australia's national security. See http://www.asio.gov.au/About/Content/what.htm.

[109] Section 10 (1), the Interception Act.

[110] Section 10, the Interception Act.

Eligible Judges and nominated Administrative Appeals Tribunal members

4.3.6 Law enforcement warrants must be issued by an eligible Judge or a nominated Administrative Appeals Tribunal (AAT) member.[111]

4.3.7 An eligible Judge refers to a Judge of a court created by the Australian Parliament who has consented to be nominated by the Attorney-General, and who has been declared by the Attorney-General to be an eligible Judge.[112] Currently, eligible Judges come from the Federal Court of Australia, the Family Court of Australia and the Federal Magistrates Service.

4.3.8 A nominated AAT member refers to a Deputy President, full-time or part-time senior member, or member of AAT who has been nominated by the Attorney-General to issue interception warrants.[113] Under section 7 of the Administrative Appeals Tribunal Act 1975, Deputy Presidents of AAT must have been legal practitioners of the High Court, Federal Court or Supreme Court of a State or Territory for not less than five years, while senior members may be legal practitioners or have expertise in other areas. Members or part-time senior members are not eligible for nomination to issue warrants unless they have the same judicial qualification as Deputy Presidents.[114] Nominated AAT members are regarded by the government as independent and being capable of assessing evidence as dispassionately as Judges.[115]

---

111 Established by the Administrative Appeals Tribunal Act 1975, AAT is empowered to conduct merit reviews on a broad range of administrative decisions made by ministers and government officials and public authorities. It also reviews administrative decisions made by some non-government bodies. Its membership consists of a President, presidential members (including Judges and Deputy Presidents), senior members and members. The President must be a Judge of the Federal Court of Australia. AAT reports to the Attorney-General. See http://www.aat.gov.au/AboutTheAAT/IntroductionToTheAAT.htm.

112 Section 6D, the Interception Act.

113 Section 6DA(1), the Interception Act.

114 Section 6DA(2), the Interception Act.

115 Tom Sherman AO (2003) p. 11. In recent years, most of the law enforcement warrants have been issued by nominated AAT members. In 2002-2003, AAT members issued 2 788 warrants which represented about 91% of the total of 3 058 warrants. The remaining warrants were issued by Family Court Judges (206 or 7%), Federal Court Judges (7 or 0.2%) and Federal Magistrates (57 or 1.9%). See Attorney-General's Department (2000), (2001), (2002), (2003) and (2004).

4.3.9 The vesting in nominated AAT members of the power to issue interception warrants derives from the concerns raised by the High Court in the Grollo case in 1995.[116] The Court held that issuing an interception warrant was not only a non-judicial power but also of intrusive and secretive nature, which could undermine the public confidence in the independence and impartiality of the Judiciary. It also held that a non-judicial function could not be conferred on a Judge without his or her consent, and that tribunals, the law officers of the Commonwealth and retired Judges were also well fitted to carry out the function of issuing warrants.

Application procedures

4.3.10 The application for national security warrants must be made by ASIO's Director-General of Security, while that for law enforcement warrants can be made by the following list of eligible authorities:[117]

(a) the Australian Federal Police;

(b) the Australian Crime Commission; or

(c) an eligible authority of a State or the Northern Territory in respect of which a Ministerial declaration is in force.[118]

4.3.11 The application for national security warrants must be made in writing setting out the reasons for which the warrant is sought and what is expected to be achieved by the issue of the warrant.

4.3.12 The application for law enforcement warrants must also be made in writing. In addition, each application must be accompanied by an affidavit setting out the facts and grounds on which the application is based, and the period for which the warrant will be in force.[119]

---

116 Bruno Grollo v. Michael John Palmer, Commissioner of the Australian Federal Police and Others F.C.95/032, http://www.newcastle.edu.au/school/law/course_resources/laws5018_media_law/aOJContempt/OJAccess/Html/aCases/Grollo95.html.

117 Sections 5, 34 and 39, the Interception Act, and Attorney-General's Department (2004) p.9.

118 The Interception Act defines eligible authorities to be the police forces of the States and of the Northern Territory. These authorities also include the Independent Commission Against Corruption, the New South Wales Crime Commission, the Police Integrity Commission, the Queensland Crime and Misconduct Commission, the Western Australian Anti-Corruption Commission, the Inspector of the Police Integrity Commission, and the Royal Commission into the Western Australian Police Service.

119 Section 42 (1), (2) and (3), the Interception Act.

Grounds on which interception warrants are issued

National security grounds

4.3.13 Before issuing a national security warrant in relation to a telecommunications service or a named person, the Attorney-General must consider some statutory criteria. In particular, the Attorney-General must be satisfied that:[120]

(a) the subject of the warrant is engaged in or reasonably suspected of being engaged in activities prejudicial to national security; or

(b) the foreign intelligence to be obtained is important to the defence of Australia or to the conduct of Australia's international affairs.

4.3.14 If the warrant application targets a named person, the Attorney-General must be further satisfied that it is necessary to intercept the communications of a person, and relying on a telecommunications service warrant to obtain the intelligence would be ineffective.

Law enforcement grounds

4.3.15 Law enforcement warrants can be issued only for the investigation of "*class 1*" and "*class 2*" offences.

4.3.16 Class 1 offences include murder, kidnapping, narcotics offences, and acts of terrorism. It also includes ancillary offences, such as aiding, abetting and conspiring, to the other class 1 principal offences.[121]

4.3.17 Class 2 offences include offences involving loss of a person's life, serious personal injury, serious arson, drug trafficking, serious frauds, bribery, corruption, money laundering, cyber-crimes, etc. In most cases, it is a requirement that the offence be punishable by imprisonment for life or at least seven years. Offences ancillary to these principal offences are also class 2 offences.[122]

4.3.18 The statutory criteria for the issue of warrants for class 1 and class 2 offences are largely the same. In particular, the eligible Judge or nominated AAT member must consider the extent to which alternative methods of investigation have been used by, or are available to, the law enforcement agency concerned.

[120] Sections 9, 9A, 11A, 11B and 11C, the Interception Act.
[121] Section 5(1), the Interception Act.
[122] Section 5D, the Interception Act.

4.3.19 The few differences in the grounds for issuing warrants are due to the fact that class 1 offences are more serious than class 2 offences.[123] The most salient difference is that before issuing a warrant for a class 2 offence, the Judge or nominated AAT member is required to consider the gravity of the offence, and the degree of interference with the privacy of any person. There is no such requirement for the issue of warrants for class 1 offences.

Duration, termination and renewal of warrants

4.3.20 The effective period for a national security warrant must not exceed six months, and the warrant may be revoked by the Attorney-General at any time before it expires.[124] The maximum period for a law enforcement warrant is 90 days, and can be extended in the same manner as an original warrant.

Lawful interception without a warrant

4.3.21 Under the Interception Act, only the Australian Federal Police or the police force of a State is allowed to conduct interception of a communication without a warrant under the following circumstances:[125]

(a) the officer or another officer of the police force is a party to the communication under interception, or the person to whom the communication is directed has consented to be intercepted;

(b) there are reasonable grounds for suspecting that another party to the communication has done an act that has resulted or may result in loss of life, serious injury or serious damage to properties; or that the person consented to be intercepted is likely to receive a communication from a person whose act has resulted or may result in loss of life, serious injury or serious damage to properties; and

(c) the need for interception must be so urgent that it is not reasonably practicable to make a warrant application.

4.3.22 After conducting the interception, the officer of the agency concerned must make an application for a warrant as soon as practicable. If the application is denied, the interception must be discontinued.

[123] Sections 45, 45A, 46 and 46A, the Interception Act.
[124] Sections 9B, 11D and 13, the Interception Act.
[125] Section 7(4) and (5), the Interception Act.

Internal safeguard measures

4.3.23 The Interception Act imposes a number of safeguards on warranted interception of telecommunications.

General Register of Warrants

4.3.24 The Commissioner of the Australian Federal Police (the Commissioner) must keep a General Register of Warrants showing the particulars of each law enforcement warrant[126], and submit the Register to the Attorney-General for inspection every three months.

Special Register of Warrants

4.3.25 The Commissioner must also keep a Special Register of Warrants showing the particulars of each warrant or renewed warrant which has failed to institute criminal proceedings against a person on the basis of intercepted information. The particulars shown are similar to those in the General Register of Warrants. The Commissioner must submit the Special Register to the Attorney-General for inspection every three months together with the General Register.

Restricted use of intercepted materials in courts

4.3.26 Under the Interception Act[127], lawfully intercepted information is not allowed to be communicated to other persons or presented as evidence in legal proceedings, subject to certain exemptions. The situations requiring exemptions include: being used in "exempt proceedings" such as prosecutions for "prescribed offences" (i.e. class 1 and class 2 offences); or being communicated to another person for a "*permitted purpose*" such as investigations into "*prescribed offences*". There are other exceptions which permit disclosure by particular persons in defined circumstances, including the interceptor, the chief officer of an agency and members of the police force.

[126] Section 81A, the Interception Act. The particulars include the following: (a) the date of issue of the warrant; (b) the Judge or nominated AAT member who issued the warrant; (c) the agency to which the warrant was issued; (d) the period for which the warrant was or is to be in force; (e) the telecommunications service to which the warrant related; (f) the name of the person specified in the warrant as a person using or likely to use the telecommunications service; and (g) each serious offence in relation to which the Judge or nominated AAT members who issued the warrant was satisfied on the application for the warrant.

[127] Sections 67, 68 and 74, the Interception Act.

Monitoring by executive authorities

Reports by the Ombudsman

4.3.27 Under the Interception Act[128], the Ombudsman[129] is required to inspect at least twice during each financial year the records of the Australian Federal Police and the Australian Crime Commission (ACC) about the issue of warrants and interception. ACC is one of the authorities eligible to apply for law enforcement warrants. One of the purposes of the inspection is to ascertain the accuracy of entries in both the General Register and Special Register of Warrants. Another purpose is to oversee the compliance with the statutory record keeping requirements of the two agencies. Within three months after the end of each financial year, the Ombudsman must report in writing to the Attorney-General about the results of the inspections. If necessary, the Ombudsman can conduct such inspections at any time and report to the Attorney-General.

4.3.28 In carrying out an inspection, the Ombudsman is empowered to, after notifying the head of the law enforcement agency concerned, enter premises occupied by the agency. The Ombudsman is entitled to full and free access to all relevant records of the agency, and make copies of or take extracts from those records. The Ombudsman can also require the head of the agency to attend a meeting before a specified inspecting officer at a specified place within a specified period or at a specified time, in order to answer questions relevant to the inspection.

Monitoring by legislature

4.3.29 The Australian Parliament has two statutory committees and two standing committees that monitor matters relating to interception of communications.

[128] Sections 79 to 89, the Interception Act.

[129] The office of the Commonwealth Ombudsman was created by the Ombudsman Act 1976. The Ombudsman is appointed by the Governor-General. The activities of the Ombudsman are governed by a number of laws, including the Telecommunications (Interception) Act 1979.

The Joint Statutory Committee on the Australian Crime Commission

4.3.30 Created by the National Crime Authority Act 1984, the Joint Statutory Committee on the Australian Crime Commission[130] has duties to examine the annual reports of ACC, and to report to the Australian Parliament on any matter relating to the performance of ACC's functions. However, the Committee is not empowered to investigate a matter relating to a relevant criminal activity, or to reconsider the findings of ACC in relation to a particular investigation.

The Parliamentary Joint Committee on ASIO, ASIS and DSD[131]

4.3.31 Legislative oversight of interception of communications conducted by intelligence and security agencies is provided by the Parliamentary Joint Committee on ASIO, ASIS and DSD, which was established under the Intelligence Services Act 2001.[132] The Committee is responsible for reviewing the administration and expenditure of the three agencies. It also reviews any matter related to the three agencies referred by the responsible Minister or a resolution of either House of the Australian Parliament. It cannot initiate a review for a matter, but can request the responsible Minister to refer a particular matter to it for review. The Committee is required to report its comments and recommendations to the Australian Parliament and the responsible Minister, and table an annual report before the Australian Parliament. However, the Committee is not allowed to inquiry into certain matters related to the three agencies, including the intelligence gathering priorities, the source of intelligence and other operational assistance or methods, particular operations, and individual complaints.

[130] The Committee consists of 10 members, namely three Members of the House of Representatives nominated by the Government Whip, two Members of the House of Representatives nominated by the Opposition Whip or by independent Members, two Senators nominated by the Leader of the Government in the Senate, two Senators nominated by the Leader of the Opposition in the Senate, and one Senator nominated by minority groups or independent Senators.

[131] ASIS (the Australian Secret Intelligence Service) is responsible for collecting overseas intelligence. DSD (the Defence Signals Directorate) is Australia's national authority for signals intelligence and information security.

[132] The Committee comprises seven members, three from the Senate and four from the House of Representatives. By convention, four members are from the parties that make up the Australian government and three from the Opposition.

The Standing Committees on Legal and Constitutional Affairs

4.3.32 The House of Representatives has a general-purpose investigatory committee known as the Standing Committee on Legal and Constitutional Affairs.[133] The Committee carries out inquiries into matters referred to it by the House or the responsible Minister. It also inquires into matters raised in annual reports of the relevant government departments, including those published by the Attorney-General, who has the power to issue interception warrants for national security purposes.

4.3.33 Compared to that of the Standing Committee on Legal and Constitutional Affairs in the House of Representatives, the mandate of the Senate Standing Committee on Legal and Constitutional Affairs is narrower. The Committee is specifically responsible for conducting inquires into a bill or part of a bill referred by the Senate. In 2004, the Committee has conducted a number of inquiries into bills relating to interception of telecommunications.

Annual reports by the Attorney-General

4.3.34 The Interception Act requires the Attorney-General to table before each House of Parliament an annual report giving details of telecommunications interception for law enforcement purposes. The report must include:[134]

(a) the number of applications for warrants and the number of warrants issued;

(b) the duration for which warrants are specified to be in force when issued, and the period for which the warrants are actually in force;

(c) the number of arrests, prosecutions and convictions based on intercepted information;

(d) the number of times when an agency intercepts a communication without a warrant in an emergency situation;

(e) the total expenditure and the average expenditure per warrant; and

(f) the availability of Judges to issue warrants and the extent to which nominated AAT members are used for that purpose.

[133] The Committee consists of 10 Members of the House, with six Members nominated by the parties that make up the Australian government and four nominated by the non-Government parties.

[134] Sections 100 to 103A, the Interception Act, and the Attorney-General's Department (2004) p.16. The Interception Act requires the information to be set out in the report for each authority eligible to apply for warrants. The information must also be set out in aggregate form to indicate in detail the extent and effectiveness of telecommunications interception.

Limit of discretion in bringing laws into operation

4.3.35 In Australia, the Prime Minister and other Ministers do not have discretion in postponing operation of an act or not bringing an act into operation. Since 1989, it has been the general practice with legislation containing a commencement clause which specifies when commencement will automatically take place. Alternatively, the commencement clause may specify when the legislation, if not proclaimed, is considered to be repealed.

4.4 Legislative amendments in relation to the "911" incident and the development of communications technology

4.4.1 In Australia, most legislative amendments made in relation to interception of communications are part of a package of counter-terrorism legislation introduced by the Australian government. Only a few provisions in those amendments are related to the development of communications technology.

The Telecommunications Interception Legislation Amendment Act 2002

4.4.2 In July 2002, the Telecommunications Interception Legislation Amendment Act 2002 (the Interception Amendment Act) was enacted. The Interception Amendment Act amended the Interception Act and extended government surveillance powers. These amendments include treating offences constituted by conduct involving acts of terrorism, child pornography and serious arson as offences in relation to which a telecommunications interception warrant may be sought.[135]

4.4.3 When the Interception Amendment Act was passed, it did not include the government proposal to extend the law enforcement agencies' power to access, without an interception warrant, the contents of "*stored*" or "*delayed access*" communications.[136] The government proposal was rejected because it was widely criticized for reducing privacy protection of communications.[137]

[135] Telecommunications Interception Legislation Amendment Bill 2002, Information and Research Services, Parliamentary Library, Department of Parliamentary Services, Bills Digest No. 121, 2001-02, p.7, and the Attorney-General's Department (2004) p 14 and (2003) pp. 9-10.

[136] They are communications that are temporarily stored in a service provider's equipment during transit, i.e. emails, voicemails, Short Message Services, etc.

[137] The Senate Legal and Constitutional Legislation Committee (2002) and Electronic Frontiers Australia (2002).

The Telecommunications (Interception) Amendment Act 2004

4.4.4 In April 2004, the Telecommunications (Interception) Amendment Act 2004 (the 2004 Act) was enacted. The 2004 Act aims to amend the Interception Act in the following aspects:[138]

New offences for interception purposes

4.4.5 The 2004 Act adds specific terrorism offences recently included in the Commonwealth Criminal Code to the list of "*class 1*" offences which has a rather general term "*acts of terrorism*" in the Interception Act. These specific terrorism offences include terrorist activities using explosive or lethal devices, providing or receiving training connected with terrorist acts, making documents likely to facilitate terrorist acts, directing the activities of a terrorist organization, and collecting funds to facilitate or engage in a terrorist act. The 2004 Act empowers law enforcement officers and ASIO officers to apply for interception warrants to investigate specific terrorist activities in Australia.

4.4.6 In addition, the 2004 Act adds various "*cyber-crime*" offences and "*dealing in firearms and armaments*" to the list of "*class 2*" offences in the Interception Act. This amendment makes it clear that an interception warrant can be issued to help the investigation of offences involving dealings in either firearms or armaments under the Interception Act.

Broader definition of "interception"

4.4.7 The 2004 Act amends the definition of "*interception*" of communications in the Interception Act to include not only "*listening and recording*" but also "*reading or viewing*", and consequently extending the prohibition against interception. This extension aims to cope with the technological advances in recent years, which have resulted in telecommunications taking the form of written words, such as emails or images, to which the concept of "*listening*" is not applicable.

[138] Telecommunications (Interception) Amendment Act 2004, No. 55 2004, http://scaleplus.law.gov.au/html/comact/11/6810/0/CM000020.htm, Telecommunications (Interception) Amendment Bill 2004, Bill Digest, No.111, 2003-04, and Telecommunications (Interception) Amendment Bill 2004, Explanatory Memorandum circulated by the Attorney-General.

Recording communications to ASIO public lines without a warrant

4.4.8 The 2004 Act introduces new provisions into the Interception Act, allowing ASIO to listen to, record, read or view telephone calls to publicly-listed ASIO telephone numbers. These numbers are telephone numbers that enable members of the public to contact ASIO, and are listed in a telephone directory or telephone number database available to the public.

Allowing interception without notifying telecommunications carriers

4.4.9 The 2004 Act amends the Interception Act by removing the requirement for ASIO to notify the telecommunications carrier where a warrant has been issued for the interception of a telecommunications service operated by the carrier and the assistance of the carrier is not required to execute the warrant. However, law enforcement agencies are still required to notify carriers when communications on their networks are intercepted, even though they do not need the assistance of the carriers.

The Telecommunications (Interception) Amendment (Stored Communications) Bill 2004

4.4.10 In June 2004, the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004 (the 2004 Bill) was passed in the House of Representatives. The 2004 Bill amends the Interception Act to exclude access to stored communications from the current prohibition against interception of communications for a period of 12 months, pending further review of access to stored communications and the contemporary relevance of Australia's interception regime by the Attorney-General's Department.

4.4.11 The 2004 Bill is the latest attempt by the Australian government to allow access to "*stored communications*" without an interception warrant. The Information and Research Services of the Parliamentary Library comments that, with the 2004 Bill, the Australian government "*is proposing an even broader exclusion, albeit temporary, from the protections*" of the Interception Act for stored communications than that criticized in the 2002 Bill.[139] On the other hand, the Australian Federal Police welcomes the 2004 Bill, noting that "*without the amendment allowing expeditious access to stored communications, highly disposable and easily destroyed forms of evidence could have been lost*" during the time taken to obtain an interception warrant.

[139] Telecommunications Interception Legislation Amendment Bill 2002, Information and Research Services, Parliamentary Library, Department of Parliamentary Services, Bills Digest No. 153, 2003-04, p.7.

4.4.12 In July 2004, the Senate Legal and Constitutional Legislation Committee recommended that the 2004 Bill be proceeded to the Senate for voting, provided that the review proposed by the Attorney-General had to be conducted and made public, and had to specifically consider the issue of whether stored communications should be exempt from the Interception Act.[140]

[140] Report of the Legal and Constitutional Legislation Committee on Provisions of the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004. The Committee presented the Report on 22 July 2004 after conducting an inquiry into the 2004 Bill.

Chapter 5 - Analysis

5.1 Introduction

5.1.1 Based on the findings in this study, the following issues are highlighted to facilitate Members' deliberation upon the regulation of interception of communications in the Hong Kong Special Administrative Region (HKSAR):

(a) the features of interception warrant systems in selected overseas jurisdictions; and

(b) the legislative amendments arising from the "911" incident and the development of communications technology in other jurisdictions.

5.1.2 These issues are discussed with reference to the relevant regulations and legislative proposal in the HKSAR, i.e. the Telecommunication Ordinance (which currently regulates interception of telecommunications), Interception of Communications Ordinance (IOCO) (which was enacted in 1997, but has not been brought into operation by the Government), and the Interception of Communications Bill (the White Bill) (which was published by the Government in February 1997 for public consultation but has not been introduced into the Legislative Council).

5.1.3 To facilitate Members' discussion, a comparison table of various features of the interception warrant systems in the three jurisdictions studied and the HKSAR is presented in Appendix I. Appendix II presents the types of interception warrant systems adopted by some other overseas places. Appendix III provides some particulars of law enforcement interceptions in the US and Australia. Appendix IV presents the charts of the number of interception warrants issued in the three selected jurisdictions.

5.2 Interception warrant systems

Legal framework

5.2.1 Among the three jurisdictions studied, both the UK and Australia use a single and overarching statute to regulate interception of communications for both law enforcement and national security purposes. Their laws also regulate interception of both actual contents of communications and non-content information of communications. On the other hand, in the US, interception for law enforcement purposes and that for national security purposes are subject to two different statutes. The former is regulated by Title III and the latter by FISA. In addition, neither Title III nor FISA covers interception of non-content information of communications, which is governed by the Pen/Trap statute.

5.2.2 In the HKSAR, both interception of communications for preventing, investigating or detecting serious crimes and that for the security of the HKSAR are regulated by a single statute, the Telecommunication Ordinance. Both IOCO and the White Bill propose a similar regulatory mode.

5.2.3 Regarding the handling of non-content information of communications, the Telecommunication Ordinance permits interception of "*any message or any class of messages*", i.e. the contents of communications, but does not cover non-content information of communications. Likewise, under the White Bill, the meaning of "*communication*" is restricted to "*the contents of a communication sent from a sender to a receiver by post or by telecommunication*".[141] However, IOCO's definition of "*communication*" includes both the contents of communications and the non-content information of communications.[142]

Issuing authority

5.2.4 Each of the three selected jurisdictions has a different issuing system for interception warrants. In the UK, all warrants are issued by the executive branch, i.e. the Home Secretary. In the US, all types of court orders authorizing interceptions within the US are issued by Judges. In Australia, depending on their purposes, warrants are issued either by the executive branch or by Judges (or professionals with judicial qualifications). As illustrated in Appendix II, the court warrant system is adopted by many overseas places.

5.2.5 In the HKSAR, under the Telecommunication Ordinance, only the head of government, i.e. the Chief Executive, can give orders to intercept communications.[143] However, IOCO proposes a new court warrant system under which interception warrants must be issued by High Court Judges. A similar system is proposed in the White Bill.[144]

---

[141] The White Bill states that it does not include "*the telephone number dialed, the address of the communication, any record maintained by the operator of the system by which the communication was sent or a communication sent through a computer network*". In addition, the White Bill does not cover communications transmitted via the computer network because such communications are sufficiently protected by a provision of the Telecommunication Ordinance, according to the Government.

[142] Under IOCO, "*communication*" includes "*telecommunication*" whose meaning is the same as that under the Telecommunication Ordinance. Section 2 of the Telecommunication Ordinance states that "*telecommunication*" refers to "*any transmission, emission or reception of communication by means of guided or unguided electromagnetic energy or both, other than any transmission or emission intended to be received or perceived directly by the human eye*". In this section, "*communication*" includes "*any communication whether between persons and persons, things and things or persons and things; and whether in the form of speech, music or other sound; or text; or visual images whether or not animated; or signals in any other form or combination of forms*".

[143] Section 33, the Telecommunication Ordinance.

[144] Section 4 (1), IOCO, and Section 9, the White Bill.

Authorization of applications

5.2.6 In all jurisdictions studied, warrant applications must be made or authorized by high-level officers. In the UK, applications must be made by or on behalf of the heads of law enforcement or intelligence agencies. In the US, Title III applications must be authorized by specified high-level officials of the Department of Justice before being approved by a Judge. FISA applications can only be authorized by the head of the Department of Justice before being approved by the FISA court. In Australia, national security warrants must be made by the head of security, and law enforcement warrants must be made by the authorities of law enforcement agencies.

5.2.7 In the HKSAR, the Telecommunication Ordinance specifies that only the head of government can order, or authorize public officers to order, interception of telecommunications. On the other hand, the proposed arrangement under IOCO is similar to those adopted in the three jurisdictions studied. Under IOCO, applications for court orders must be made by police officers of or above the level of superintendent, or senior officers of other law enforcement agencies.[145] The White Bill also proposes that only public officers of not less than directorate rank or equivalent authorized by the head of government can apply for warrants.[146]

5.2.8 It is noteworthy that, among the jurisdictions studied, only the US requires court order applications to be authorized by judicial officers. In the UK and Australia, as well as in the HKSAR, judicial officers are not involved in the application process or the authorization of applications.

Grounds on which warrants are issued

Less specific requirements for applications for national security warrants

5.2.9 In all three jurisdictions studied, the major requirements for applications for national security warrants are less specific than those for law enforcement warrants. In the UK, the types of serious offences under investigation eligible for the issue of law enforcement warrants are defined, but the interests of national security or the economic well-being that national security warrants seek to safeguard are not defined. In the US, Title III applications must demonstrate that there is probable cause to believe that communications concerning a particular offence have to be obtained through the interception authorized, but FISA applications are not required to do so. In Australia, to issue law enforcement warrants, the issuing authorities must consider whether the information to be intercepted is for the investigation of a specified offence. However, the requirement is much looser for issuing national security warrants.

[145] Section 5 (1) and (2), IOCO.
[146] Section 5, the White Bill.

5.2.10 In the HKSAR, under the Telecommunication Ordinance, whenever the head of government determines that the public interests, which are not defined, so require, he can order an interception operation. In contrast, both IOCO and the White Bill set out more specific requirements for the issue of warrants.[147]

Use of alternative methods

5.2.11 In the jurisdictions studied, the application for law enforcement warrants for the investigation of serious crimes is required to prove the extent to which alternative methods of investigation have been used by, or are available to, the intercepting agencies. However, this ground is not regarded by all three jurisdictions as a must in the consideration of the issue of warrants for national security purposes. Only the UK requires the application to prove that the information sought could not reasonably be obtained by other means. There is no similar requirement for the application for FISA warrants in the US or for national security warrants in Australia. In the HKSAR, the practices proposed under IOCO and the White Bill are similar to that adopted in the UK.

Duration, termination and renewal of warrants

5.2.12 All three jurisdictions studied have a limit on the length of duration for interception warrants. In the UK, all warrants, except those for urgent cases, have the same initial effective period of up to 30 days, regardless of what they seek to achieve. In the US and Australia, different types of warrants have initial effective periods of different length, with the warrants for national security purposes being the longest. In the US, Title III warrants can last for not more than 30 days. Pen/Trap warrants are given a longer effective period of not more than 60 days. The effective period of FISA warrants is the longest, which is up to one year. In Australia, the maximum period for law enforcement warrants is 90 days, and six months for national security warrants.

[147] Under Section 6 of the White Bill, a warrant can only be issued "*for preventing, investigating or detecting serious crime*" where there is reasonable cause to believe that the interception is "*likely to uncover useful information*" leading to a suspect or an arrest in respect of serious crimes, or "*for the security of Hong Kong*" where the interception is "*likely to be of substantial value*" in furthering the purpose. The requirements set out in IOCO are more specific than those under the White Bill. Under Section 4 (2) and (3) of IOCO, a court order must not be made unless it is "*necessary for the purpose of preventing or detecting a serious crime; or in the interest of the security of Hong Kong*". The Judge must also have reasonable grounds to believe that an offence is being committed, has been committed or is about to be committed; and that information about the offence will be obtained through the interception sought. There is also good reason to believe that the interception will result in a conviction.

5.2.13 In the HKSAR, the Telecommunication Ordinance does not set any limit on the length of duration for interception warrants. Under IOCO,[148] court orders are valid for a period not exceeding 90 days. The White Bill proposes that warrants should be issued for an initial period not exceeding six months.[149]

Internal safeguard measures

5.2.14 The intercepting agencies in the three selected jurisdictions have internal safeguards against misuse of warranted interception of communications. In the UK, the intercepting agencies are required to satisfy minimization obligations to restrict the disclosure, copying, retention and destruction of intercepted materials. In the US and Australia, similar safeguards are imposed on materials intercepted under court orders. Australia is the only place where the head of the federal police is required to keep registers showing the particulars of each law enforcement warrant, including information on each warrant or its renewal which has failed to incriminate the interception subject.

5.2.15 In the HKSAR, the Telecommunication Ordinance does not provide any safeguard for intercepted materials. On the other hand, both IOCO and the White Bill propose to devise administrative arrangements to limit the disclosure of intercepted materials.[150]

Executive monitoring

5.2.16 Among the jurisdictions studied, only Australia empowers the Ombudsman to oversee and inspect the law enforcement authorities' compliance with the statutory record keeping requirements regarding the use of interception warrants. Both the UK and the US attach more importance to the judicial mechanism to enforce compliance with interception laws. In the HKSAR, the Ombudsman does not have a role in urging the executive branch to meet the record keeping requirements under the Telecommunication Ordinance, IOCO or the White Bill. Nevertheless, IOCO and the White Bill attach more importance to the legislature and the judiciary respectively to monitor the record keeping requirements for the interception agencies.

[148] Section 6 (4), (5) and (6), IOCO.
[149] Section 8, the White Bill.
[150] Section 8, IOCO, and section 10, the White Bill.

Monitoring by judiciary

5.2.17 Among the three jurisdictions under study, only Australia does not have a judicial mechanism monitoring the issue of interception warrants. In the UK, the post of the Interception of Communications Commissioner, which must be held by a person with high judicial office, is established to oversee the use of interception powers. In the US, the issuing Judge of a Title III warrant is required to file a written report with the Director of the Administrative Office of the US Courts on each warrant application. Law enforcement agencies must also submit annual reports on their interception activities to the Administrative Office.

5.2.18 In the HKSAR, there is no Interception of Communications Commissioner or any equivalent post under the Telecommunication Ordinance. A similar monitoring setup does not exist under IOCO either. On the other hand, the White Bill proposes to establish a Supervisory Authority (SA) who must be a Justice of Appeal and appointed by the head of government from among nominations submitted by the Chief Justice.[151] Most of the roles of the proposed SA post are similar to those of the Interception of Communications Commissioner in the UK.[152]

5.2.19 A major difference between SA and the Interception of Communications Commissioner is that SA is empowered to receive and examine complaints from members of the public who believe that their communications have been intercepted.[153] If a contravention is found to have occurred, SA has power to quash the relevant warrant, direct the destruction of the intercepted materials and order compensation to the complainant. In the UK, the power to hear and determine complaints rests with the Investigatory Powers Tribunal.

---

[151] Sections 12 and 13, the White Bill.

[152] Similar to the Interception of Communications Commissioner in the UK, SA: (a) must have held high judicial office and is appointed by the head of government; (b) has the functions of keeping under review the issue and proper execution of warrants, and reviewing the adequacy of safeguards for intercepted materials; (c) can require relevant parties to provide all necessary documents or information when carrying out his/her statutory functions; and (d) must submit annual reports to the head of government, and the reports are subsequently laid before the legislature.

[153] Sections 12 to 14, the White Bill. SA's scope of examination is confined to ascertaining whether the interception, if any, has been authorized by a warrant and any interception law has been contravened. When examining a complaint, SA has access to all official documents relating to the warrant and the application for the warrant, including the materials intercepted. Besides, public officers are placed under a duty to provide SA with information. SA is required to conduct an examination in private. The decision of SA is not subject to appeal or liable to be questioned in any court.

Monitoring by legislature

Parliamentary committees

5.2.20 The three jurisdictions under study all have parliamentary committees to monitor matters relating to interception of communications. In the UK, the Intelligence and Security Committee oversees the expenditure, administration and policies relating to interception for national security purposes only. On the other hand, the US and Australia have parliamentary committees to monitor matters relating to interception for both law enforcement and national security purposes.

5.2.21 In the US, the Committee on the Judiciary and Intelligence of the House of Representatives oversees the operation of the Title III warrant system. In addition, the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence are specifically concerned with foreign intelligence surveillance.

5.2.22 In Australia, monitoring by the legislature is mainly conducted by two statutory committees, namely the Joint Statutory Committee on the Australian Crime Commission, which oversees interception relating to law enforcement, and the Parliamentary Joint Committee on ASIO, ASIS and DSD, which is solely concerned with national security matters.

5.2.23 In the HKSAR, the Telecommunication Ordinance does not provide for any mechanism for the legislature to monitor the use of interception powers by the head of government. Neither the White Bill nor IOCO provides for a committee in the legislature to which the intercepting agencies are accountable. Nevertheless, IOCO empowers the Legislative Council to require at any time the Secretary for Security to provide specific information on interceptions for any specified period. The White Bill only proposes the head of government to table annual reports concerning the issue of interception warrants in the Legislative Council.[154]

Reports to the legislature

5.2.24 Interception laws in the three selected jurisdictions all require the monitoring authorities to submit to the legislature annual reports on interceptions for law enforcement purposes. In the UK, the Interception of Communications Commissioner must submit annual reports to the Prime Minister, and the reports are then laid before Parliament. In the US, the Director of the Administrative Office of the US Courts must submit annual wiretap reports to Congress. In Australia, the Attorney-General is required to table annual reports on telecommunications interceptions before the Australian Parliament.

[154] Section 14, the White Bill.

Public Disclosure of information about interceptions

5.2.25 The extent to which information about interceptions is publicly disclosed by the monitoring authorities in the three selected jurisdictions varies. In the UK, the annual reports prepared by the Interception of Communications Commissioner merely disclose the overall number of warrants issued. In the US and Australia, as shown in Appendix III, the disclosure of information is more specific and substantive, which includes not only the number of warrant applications requested and authorized, but also the average duration of original and renewed warrants issued, the number of arrests and convictions on the basis of intercepted materials, and the expenses related to warrants.

5.2.26 In all the jurisdictions studied, the information on interceptions disclosed to the public is mostly about law enforcement rather than national security, as shown in Appendix IV. In the UK, the Interception of Communications Commissioner's annual reports do not contain any specific figures about interception for national security or economic well-being purposes. In the US, FISA annual reports merely disclose the overall number of interceptions and physical searches. In Australia, no information about the applications for and execution of national security warrants is provided in the Attorney-General's annual reports which are made available to the public.

5.2.27 In the HKSAR, the Telecommunication Ordinance has no provisions on public disclosure of interceptions. As proposed under IOCO, the information about interceptions disclosed to the legislature is similar to that in the US and Australia,[155] except that it does not cover the expenses related to warrants. The White Bill only requires the disclosure of the number of warrants authorized and their average length and extensions.[156]

5.3 Legislative amendments in relation to the "911" incident and the development of communications technology

5.3.1 In the three selected jurisdictions, most recent legislative amendments made in relation to interception of communications have arisen from the "911" incident rather than the development of communications technology. In general, the "911" incident has prompted the three jurisdictions to confer more investigatory powers upon law enforcement and security authorities.

---

[155] Under section 11 of IOCO, the information on interceptions disclosed to the Legislative Council comprises: (a) the number of interceptions authorized and denied; (b) the nature and location of the facilities and the place where communications have been intercepted; (c) the major offences for which interception has been used; (d) the types of interception methods used; (e) the number of persons arrested and convicted as a result of interceptions, (f) the average duration of each interception; and (g) the number of renewals sought and denied.

[156] Section 14, the White Bill.

5.3.2 In the UK, the recently enacted Anti-terrorism, Crime and Security Act requires CSPs to keep their customers' communications data for national security purposes. CSPs are also required to provide assistance to intercepting agencies in giving effect to interception warrants. In addition, the Interception of Communications Code of Practice has been issued to facilitate the compliance of the intercepting agencies with laws.

5.3.3 In the US, the PATRIOT Act has made significant changes to interception laws. For instance, law enforcement agencies and intelligence agencies are encouraged to share intercepted materials, and more terrorism offences can be investigated under Title III interception warrants.

5.3.4 In Australia, a number of significant legislative amendments to the Interception Act have been regarded by the government as part of a package of counter-terrorism measures. Under the amendments, terrorism offences are permitted to be investigated under interception warrants. The definition of "interception" is also broadened, so that electronic messages or images can be lawfully intercepted in the event of terrorism offences.

Appendix I

A comparison of the warrant systems for interception of communications in the HKSAR, the UK, the US and Australia

	Types of warrants	Issuing authorities
HKSAR	• No special classification of warrants.	• Under the Telecommunication Ordinance, all interceptions are ordered by the head of government; and • Both IOCO and the White Bill propose that all interception orders are issued by High Court Judges.
UK	• Normal warrants specify a person or a single set of premises; and • Certificated warrants apply solely to external communications outside the UK.	• All warrants are issued by the Home Secretary.
US	• Title III court orders authorize interception of contents of communications for law enforcement purposes; • FISA court orders authorize interception of contents of communications of foreign powers and their agents within the US for national security purposes; and • Pen/Trap court orders are issued to intercept non-content information of communications.	• Title III and Pen/Trap orders are issued by Judges of US District Courts or US Court of Appeals; and • FISA orders are issued by the FISA Court.
Australia	• Law enforcement warrants are issued for law enforcement purposes; and • National security warrants are issued for national security purposes.	• National security warrants are issued by the Commonwealth Attorney-General or the Director-General of Security; and • Law enforcement warrants are issued by eligible Judges or nominated Administrative Appeals Tribunal members.

Appendix I (cont'd)

	Application procedures	Major grounds on which warrants are issued
HKSAR	• Under the Telecommunication Ordinance, only the head of government can order, or authorize any public officer to order, interception; • IOCO proposes that applications must be made by senior law enforcement officers; and • The White Bill proposes that only public officers of not lower than directorate rank or equivalent authorized by the head of government can apply for warrants.	• Under the Telecommunication Ordinance, whenever the head of government considers that the public interest requires; • IOCO proposes that court orders are required for preventing or detecting serious crimes or in the interest of the security of the HKSAR; and • The White Bill proposes that a warrant can be issued only for the purpose of preventing, investigating or detecting serious crimes, or the security of the HKSAR.
UK	• Applications must be made by the heads of law enforcement or security agencies.	• Warrant applications must meet the "*necessity*" and "*proportionality*" tests.
US	• Title III and FISA applications must be authorized by high-level judicial officials. Pen/Trap applications can be made by any attorney for the federal government.	• Title III and FISA applications must meet the "*probable cause*" test, while Pen/Trap applications are not required to do so.
Australia	• Applications for law enforcement warrants must be made by eligible authorities. Applications for national security warrant can be made only by the Director-General of Security.	• Law enforcement warrants can be issued only for the investigation of specified offences. National security warrants can be issued when the interception subjects may engage in activities prejudicial to national security or the information to be obtained is important to the national security of Australia.

Appendix I (cont'd)

	Duration and renewal of warrants	Disclosure and admissibility of evidence
HKSAR	• The Telecommunication Ordinance has no provisions about these topics; • IOCO proposes that new court orders are valid for up to 90 days, and they can be renewed once for a period of up to 90 days; and • The White Bill proposes that new warrants are valid for up to six months, and there is no upper limit on the number of renewals made.	• The Telecommunication Ordinance has no provisions about these topics; • IOCO proposes that lawfully intercepted materials are admissible as evidence in court; and • The White Bill proposes that intercepted materials are not admissible as evidence in court, unless they are used to prove an illegal interception.
UK	• New warrants are valid for up to three months; and • Warrants can be renewed successively. Each renewal on serious crime grounds is valid for up to three months. Each renewal on national security or national economic well-being grounds is valid for six months.	• Intercepted materials are not admissible as evidence in court, except in limited circumstances.
US	• New Title III orders, new FISA orders and new Pen/Trap orders are valid for up to 30 days, 90 days, and 60 days respectively; and • All the three types of orders can be renewed successively for the same duration as their original orders.	• Lawfully intercepted materials are admissible as evidence in court.
Australia	• New law enforcement warrants are valid for up to 90 days and new national security warrants up to six months; and • Each type of warrants can be renewed successively for the same duration as their original orders.	• Lawfully intercepted materials are admissible as evidence in specified proceedings or circumstances.

Appendix I (cont'd)

	Monitoring by executive authorities	Monitoring by judiciary
HKSAR	• No statutory mechanism for monitoring by the executive authorities is provided by the Telecommunication Ordinance, IOCO or the White Bill.	• The White Bill proposes to set up a Supervisory Authority, who is a Justice of Appeal and appointed by the head of government.
UK	• No statutory mechanism for monitoring by the executive authorities is provided by RIPA.	• The use of interception powers by intercepting agencies is monitored by the Interception of Communications Commissioner who is appointed by the Prime Minister and is a serving or retired Judge.
US	• No statutory mechanism for monitoring by the executive authorities is provided by the three interception statutes.	• Under Title III, the Judge who issues or denies a court order must report to the Administrative Office of the US Courts (the Administrative Office). Prosecutors must also submit annual reports to the Administrative Office providing information on their applications for court orders during the previous year; • Under FISA, the Attorney General must submit annual reports to the Administrative Office providing brief information on the issue of FISA warrants; and • Under the Pen/Trap statute, if a Pen/Trap device is used with any wiretap devices, such use must be reported to the Administrative Office.
Australia	• The Ombudsman is required to inspect at least twice every year the records of warrants maintained by the Australian Federal Police and the Australian Crime Commission, and report to the Attorney-General on the results of the inspections.	• No statutory mechanism for monitoring by the judiciary is provided by the Interception Act.

Appendix I (cont'd)

	Monitoring by legislature	Monitoring by public
HKSAR	• The Telecommunication Ordinance does not provide for any mechanism for monitoring by the legislature; • IOCO proposes that the Legislative Council can require the Secretary for Security to provide information on interceptions conducted by the Government; and • The White Bill proposes that the head of government tables annual reports concerning the issue of interception warrants in the Legislative Council.	• No statutory mechanism for monitoring by the public is provided by the Telecommunication Ordinance, IOCO or the White Bill.
UK	• The expenditure, administration and policies relating to interception of communications conducted by security agencies are monitored by a statutory parliamentary committee known as the Intelligence and Security Committee. The Committee reports annually to the Prime Minister who tables the report in Parliament; and • The Interception of Communications Commissioner must submit annual reports to the Prime Minister who then tables the reports in Parliament.	• Members of the public who are aggrieved by interception activities can lodge complaints with the Investigatory Powers Tribunal, which can hear and determine complaints, award compensation and quash warrants.
US	• The Administrative Office must submit annual reports to Congress providing information on the particulars of Title III warrants; • The Attorney General must submit annual FISA reports to Congress, and fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence concerning surveillance under FISA twice every year; and • The Attorney General must submit annual reports on the particulars of Pen/Trap warrants to Congress.	• No statutory mechanism for monitoring by the public is provided by Title III, FISA or the Pen/Trap statute.
Australia	• The Joint Statutory Committee on the Australian Crime Commission has duties to examine the annual reports of the Australian Crime Commission (ACC), which can apply for interception warrants for law enforcement purposes, and to report to the Australian Parliament on the performance by ACC; and • The Parliamentary Joint Committee on ASIO, ASIS and DSD monitors the interceptions conducted by intelligence and security agencies.	• No statutory mechanism for monitoring by the public is provided by the Interception Act.

Appendix II

Types of interception warrant systems adopted by some overseas places

Places where interception warrants are issued by executive authorities	Places where interception warrants are issued by courts	Places where interception warrants are issued by executive authorities or courts
Republic of India	Argentine Republic	Kingdom of Thailand
Republic of Singapore	Belgium	Republic of Bulgaria
	Canada	Republic of Poland
	Czech Republic	Republic of Hungary
	French Republic	State of Israel
	Federal Republic of Germany	
	Greece	
	Italian Republic	
	Kingdom of the Netherland	
	Kingdom of Spain	
	New Zealand	
	Republic of Finland	
	Republic of Iceland	
	Republic of the Philippines	
	Switzerland	

Source: Privacy and Human Rights: An International Survey of Privacy Laws and Practice (2003).

Appendix III

Particulars of court orders for law enforcement purposes in the US (1996-2003)

	1996	1997	1998	1999	2000	2001	2002	2003
Number of applications for court orders	1 150	1 186	1 331	1 350	1 190	1 491	1 359	1 442
Number of applications for court orders denied/withdrawn	1	0	2	0	0	0	1	0
Number of court orders issued	1 149	1 186	1 329	1 350	1 190	1 491	1 358	1 442
Average days of original court orders issued	28	28	28	27	28	27	29	29
Number of renewed court orders issued	887	1 028	1 164	1 367	926	1 008	889	1 145
Average days of renewed court orders issued	28	28	27	29	28	29	29	29
Number of arrests on the basis of lawfully intercepted information	2 464	3 086	3 450	4 372	3 411	3 683	3 060	3 674
Number of convictions in which lawfully intercepted information given in evidence	502	542	911	654	736	732	493	843

Source: Wiretap annual reports published by the Administrative Office of the US Courts.

Appendix III (cont'd)

Particulars of warrants for law enforcement purposes in Australia (1996-2003)

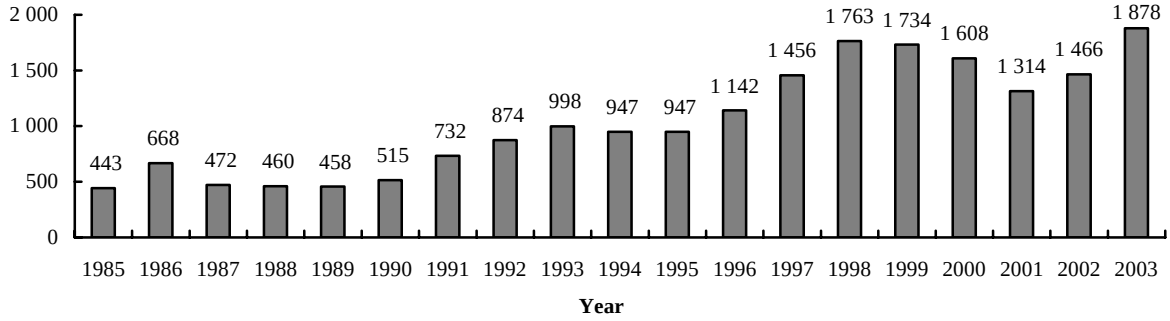
	96/97	97/98	98/99	99/00	00/01	01/02	02/03
Number of applications for warrants	638	684	1 286	1696	2 164	2 518	3 067
Number of applications for warrants denied/ withdrawn	11	9	2	7	7	4	9
Number of warrants issued	627	675	1 284	1 696	2 157	2 514	3 058
Average days of original warrants issued	44.02	50.24	39.25	37.09	48.18	47.87	44.28
Number of renewed warrants issued	137	109	198	270	309	462	736
Average days of renewed warrants issued	52.65	43.08	50.85	53.18	60.44	66.95	51.52
Number of arrests on the basis of lawfully intercepted information	493	625	633	1109	1 033	1 479	1 535
Number of convictions in which lawfully intercepted information given in evidence	360	330	713	691	623	935	1 125

Source: Interception Act annual reports published by the Australian Government Attorney-General's Department.

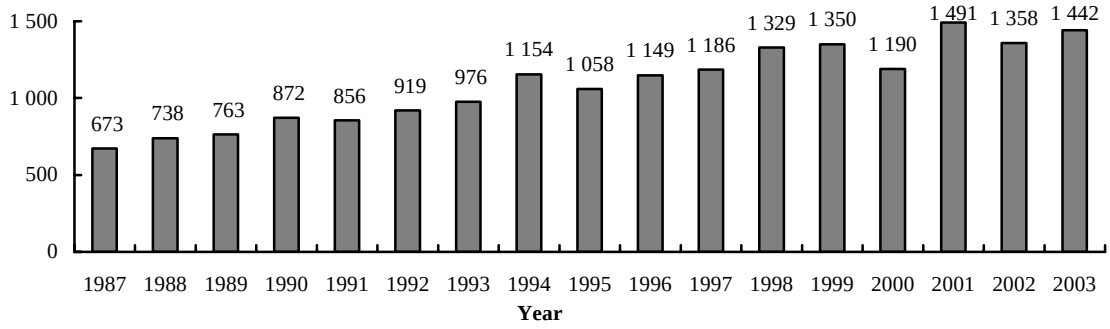
Appendix IV

Figures 1 - Interception warrants issued in the UK, the US and Australia

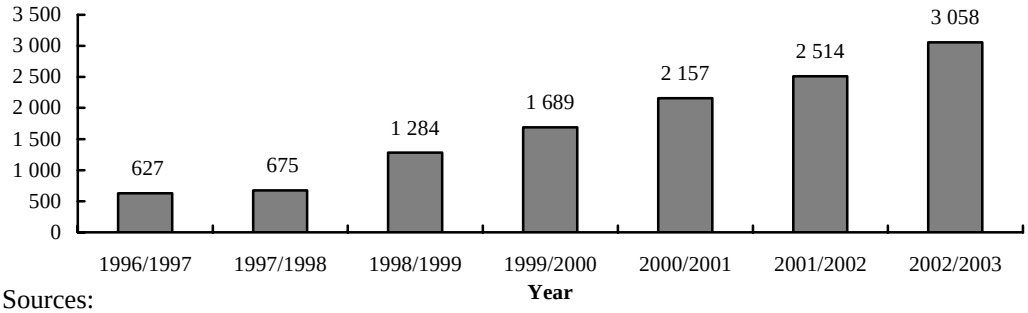
UK – Only the combined figures of all interception warrants (including those issued for law enforcement and national security purposes) in England and Wales are disclosed by the monitoring authorities.



US – Only the figures of Title III warrants are fully disclosed by the monitoring authorities.



Australia – Only the figures of law enforcement warrants are disclosed by the monitoring authorities.



Sources:

(a) Annual reports published by the Interception of Communications Commissioner of the UK;
(b) Wiretap annual reports published by the Administrative Office of the US Courts;
(c) FISA annual reports submitted by the Department of Justice to the Administrative Office of the US Courts; and
(d) Interception Act annual reports published by the Australian Government Attorney-General's Department.

References

The United Kingdom

1. *Anti-terrorism, Crime and Security Act 2001*. Available from: http://www.legislation.hmso.gov.uk/acts/acts2001/10024--b/htm/ [Accessed January 2005].

2. Broadbrige, Sally. (2001) *The Anti-Terrorism, Crime and Security Bill: Introduction and Summary*. Research Paper 01/101. Available from: http://www.publications.parliament.uk/ [Accessed January 2005].

3. Cyber-rights and Cyber-liberties. *Recent Interception of Communications related to Legal and Policy Developments*. Available from: http://www.cyber-rights.org/interception/ [Accessed January 2005].

4. Danby, Grahame. (2002) *Communications Data: Access and Retention.* Research Paper 02/63. House of Commons Library. Available from: http//www.parliament.uk/parliamentary_publications_and_archives/researchpapers.cfm/ [Accessed January 2005].

5. *European and National Law.* The STOA Program, Directorate A, Directorate General for Research, European Parliament.

6. *Explanatory Notes to Anti-Terrorism, Crime and Security 2001*. Available from: http://www.legislation.hmso.gov.uk/acts/en2001/2001en24.htm/ [Accessed January 2005].

7. *Intelligence and Security Committee Annual Report 2003-2004.*

8. *Intelligence Services Act 1994.* Available from: http://www.legislation.hmso.gov.uk/acts/acts1994/Ukpga_19940013_en_1.htm/ [Accessed January 2005].

9. *Olmstead v. United States, 277 U.S. 438 (1928), Docket No: 493.* Available from: http://www.oyez.org/oyez/resource/case/288/ [Accessed January 2005].

10. *Regulation of Investigatory Powers Act 2000.* Available from: http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm/ [Accessed January 2005].

11. *Regulation of Investigatory Powers Bill. House of Commons Standing Committee Debates.* 14 March 2000. Available from: http://www.publications.parliament.uk/ [Accessed January 2005].

12. *Regulation of Investigatory Powers Bill. House of Commons Standing Committee Debates.* 28 March 2000. Available from: http://www.publications.parliament.uk/ [Accessed January 2005].

13. *Regulation of Investigatory Powers Bill. House of Commons Standing Committee Debates.* 30 March 2000. Available from: http://www.publications.parliament.uk/ [Accessed January 2005].

14. *Regulation of Investigatory Powers Bill. House of Commons Standing Committee Debates.* 4 April 2000. Available from: http://www.publications.parliament.uk/ [Accessed January 2005].

15. *Regulation of Investigatory Powers Bill. House of Commons Standing Committee Debates.* 6 April 2000. Available from: http://www.publications.parliament.uk/ [Accessed January 2005].

16. *Report of the Interception of Communications Commissioner for 2003.*

17. *Report of the Interception of Communications Commissioner for 2002.*

18. *Report of the Interception of Communications Commissioner for 2001.*

19. The Home Office. (1999) *Interception of Communications in the United Kingdom:* A Consultation Paper. Available from:http://www.homeoffice.gov.uk/docs/interint.html/ [Accessed January 2005].

20. The Home Office. (2002) *Interception of Communications Code of Practice.*

The United States

1. American Civil Liberties Union. *Surveillance under the USA PATRIOT Act.* Available from:http://www.aclu.org/ [Accessed January 2005].

2. Annual Reports submitted by the U.S. Department of Justice to the Administrative Office of the United States Courts pursuant to the Foreign Intelligence Surveillance Act of 1978, 1997-2004.

3. Boucher, Sarah, et al. (2001) *Internet Wiretapping and Carnivore.* Available from: http://www.google.com.hk/ [Accessed January 2005].

4. Bulzomi, Michael J. (2003) *Foreign Intelligence Surveillance Act: Before and After the USA PATRIOT Act.* Available from: http://www.fbi/publications/leb/2003/june2003/june03leb.htm/ [Accessed January 2005].

5. Centre for Democracy and Technology (2004). *The Nature and Scope of Governmental Electronic Surveillance Activity.* Available from: http://www.cdt.org/wiretap/wiretap_overview.html/ [Accessed January 2005].

6. *Child Sex Crimes Wiretapping Act of 2002.*

7. Collins, Jeffrey G. (2003) *Questions and Answers about the USA PATRIOT ACT*. Available from: http://www.usdoj.gov/usao/mie/ctu/FAQ_Patriot.htm/ [Accessed January 2005].

8. Doyle, Charles. (2002) *The USA PATRIOT Act: A Legal Analysis.* Congressional Research Service, the Library of Congress, 15 April 2002.

9. Doyle, Charles. (2004) *USA PATRIOT Act Sunset: A Sketch.* Congressional Research Service, the Library of Congress, 7 January 2004.

10. Foreign Intelligence Surveillance Act. US Code Collection, Title 50, Chapter 36, Subchapter I, Section 1801–1811. Available from: http://www4.law.cornell.edu/ [Accessed January 2005].

11. Freeh, Louis J. (2000) *Cybercrime*. Testimony submitted to the Senate Committee on Appropriations Subcommittee for the Departments of Commerce, Justice, State, the Judiciary, and Related Agencies. 16 February 2000. Available from: http://www.fbi.gov/congress/congress00/cyber021600.htm/ [Accessed January 2005].

12. Galemore, Gary L. (2000) *Congressional Overrides of Presidential Vetoes*. Congressional Research Service, the Library of Congress, 2 November 2000.

13. Gallagher, Francis A.(2001) *Limited Expansion of the Predicate Offences for Title III Electronic Surveillance.* Available from: http://www.fbi.gov/congress/congress01/gallagher062101.htm/ [Accessed January 2005].

14. IIT Research Institute. (2000) *Independent Review of the Carnivore System – Final Report.*

15. Kennedy, Charles H. and Swire, Peter P. *State Wiretaps and Electronic Surveillance After September 11*.

16. Kerr, Donald M. (2000) *Carnivore Diagnostic Tool.* Testimony presented before the United States Senate, the Committee on the Judiciary. Available from: http://www.fbi.gov/congress/congress00/kerr090600.htm/ [Accessed January 2005].

17. Kerr, Donald M. (2000) Congressional Statement presented before the Committee on the Judiciary Subcommittee on the Constitution, the United States House of Representatives Available from: http://www.house.gov/ [Accessed January 2005].

18. Knowlton, David R. (2000) *Electronic Surveillance.* Testimony made before the House Judiciary Committee, Subcommittee on Crime.

19. Mueller, Robert S. (2004) Congressional statement presented before the National Commission on Terrorist Attacks upon the United States. Available from: http://www.fbi.gov/congress/congress04/mueller041404.htm/ [Accessed January 2005].

20. Regini, Lisa A. (1997) *Searching Pagers Incident to Arrest.* Law Enforcement Bulletin, FBI Publications. Available from:http://www.fbi.goc/publications/leb/1997/jan977.htm/ [Accessed January 2005].

21. Rundquist, Paul S. (1999) *Engrossment, Enrollment, and Presentation of Legislation*. Congressional Research Service, the Library of Congress, 2 March 1999.

22. Schott, Richard G. (2003) *Warrantless Interception of Communications: When, Where, and Why It Can be Done.* Available from:http://www.fbi.gov/publications/leb/2003/jan2003/jan03leb.htm/ [Accessed January 2005].

23. The Attorney General. (2002a) *Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of a Criminal Investigation.*

24. The Attorney General. (2002b) *Guidelines Regarding Prompt Handling of Reports of Possible Criminal Activity Involving Foreign Intelligence Sources.*

25. The Attorney General. (2002c) *Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral Interception Information Identifying United States Persons.*

26. The Pen/Trap provisions. US Code Collection, Title 18, Part II, Chapter 206, Section 3121–3127. Available from: http://www4.law.cornell.edu/ [Accessed January 2005].

27. *The United States Constitution.* Available from: http://www.house.gov/Constitution/Constitution.html/ [Accessed January 2005].

28. *Title III of the Omnibus Crime Control and Safe Streets Act of 1968.* US Code Collection, Title 18, Part I, Chapter 119, Section 2510–2522. Available from: http://www4.law.cornell.edu/ [Accessed January 2005].

29. *U.S. Constitution: Fourth Amendment.* Available from: http://www.caselaw.1p.findlaw.com/data/constitution/amendment04/index.html. [Accessed January 2005].

30. United States Department of Justice. (2002) *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.* Available from: http://www.cybercrime.gov/s&smanual2002.htm/ [Accessed January 2005].

31. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*. Available from: http://thomas.loc.gov/ [Accessed January 2005].

32. Wiretap Reports. 1998-2003. Administrative Office of the United States Courts. Available from: http://www.uscourts.gov/ [Accessed January 2005].

Australia

1. Australian Communications Authority. (2000) *Internet Service Providers Interception Obligations.* Available from: http://www.aca.gov.au/ [Accessed January 2005].

2. Australian Labour Party. (2002) *More Telephone Taps in Australian than the United States.* Available from: http://www.alp.org.au/media/0902/20002179.html/ [Accessed January 2005].

3. Branch, Philip. (2003) *Lawful Interception of the Internet.* Issue 1: Spring 2003, Australian Journal of Emerging Technologies and Society. Available from: http://www.swin.edu.au/ajets/ [Accessed January 2005].

4. Ford, Peter. (1999) *Telecommunications Interception Policy Review.* Information and Security Law Division, Attorney-General's Department, the Government of Australia.

5. Hancock, Nathan. (2002) *Terrorism: Legislating for Security.* Research Note No. 25, 2001-02. Available from: http://www.aph.gov.au/library/pubs/rn/2001-02/02rn25.htm/ [Accessed January 2005].

6. Hancock, Nathan. (2002a) *Terrorism and the Law in Australia: Legislation, Commentary and Constraints.* Research Paper No. 12. Available from: http://www.aph.gov.au/library/pubs/rp/2001-02/02rp12.htm/ [Accessed January 2005].

7. Hancock, Nathan. (2002b) *Terrorism and the Law in Australia: Supporting Materials.* Research Paper No. 13. Available from: http://www.aph.gov.au/library/pubs/rp/2001-02/02rp13.htm/ [Accessed January 2005].

8. *Overview of Bill and Effect on Existing Privacy Protections.* Available from: http://www.efa.org.au/Issues/Privacy/tia_bill2002.html/ [Accessed January 2005].

9. *Surveillance Devices Bill (No.2) 2004.* Bills Digest No.24 2004-05. Information and Research Services, Parliamentary Library, Department of Parliamentary Services.

10. *Telecommunications (Interception) Act 1979 Report for the year ending 30 June 1999.*

11. *Telecommunications (Interception) Act 1979 Report for the year ending 30 June 2000.*

12. *Telecommunications (Interception) Act 1979 Report for the year ending 30 June 2001*.

13. *Telecommunications (Interception) Act 1979 Report for the year ending 30 June 2002*

14. *Telecommunications (Interception) Act 1979 Report for the year ending 30 June 2003.*

15. *Telecommunications (Interception) Act 1979.* Available from: http://scaleplus.law.gov.au/html/pasteact/0/464/top/htm/ [Accessed January 2005].

16. *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004 – Question on Notice and Supplementary Submission.* Available from: http://www.privacy.gov.au/publications/senTIAsup.html/ [Accessed January 2005].

17. *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004.* Bills Digest, No. 153 2003-04. Information and Research Services, Parliamentary Library, Department of Parliamentary Services. Available from: http://www.aph.gov.au/publications/index.htm/ [Accessed January 2005].

18. *Telecommunications (Interception) Amendment Act 2004.* No.55. Available from:http://scaleplus.law.gov.au/html/comact/11/6810/0/CM000020.htm/ [Accessed January 2005].

19. *Telecommunications (Interception) Amendment Bill 2004.* Bills Digest, No. 111 2003-04. Information and Research Services, Parliamentary Library, Department of Parliamentary Services.

20. The Senate. (2004) *Legal and Constitutional Legislation Committee. Provisions of the Telecommunications (Interception) Amendments (Stored Communications) Bill 2004.*

Hong Kong Special Administrative Region

1. *Interception of Communications Ordinance.* Available from: http://www.justice.gov.hk/ [Accessed January 2005].

2. Ng, Hon Wah. (2003) *Remedies Against Telephone Tapping by the Government.* Hong Kong Law Jorunal, Vol. 33, Part 3. Sweet & Maxwell Asia, pp. 543-567.

3. *Post Office Ordinance.* Available from: http://www.justice.gov.hk/ [Accessed January 2005].

4. Security Branch. (1997) *Consultation Paper on Interception of Communications Bill.*

5. *Telecommunication Ordinance.* Available from: http://www.justice.gov.hk/ [Accessed January 2005].

6. The Law Reform Commission of Hong Kong. (1996) *Report on Privacy: Regulating the Interception of Communications.*

Others

1. Cameron, Iain. (2000) *National Security and the European Convention on Human Rights*. Kluwer Law International, the Netherland.

2. Electronic Surveillance Task Force of the Digital Privacy and Security Working Group. (1997) *Communications Privacy in the Digital Age. Centre for Democracy and Technology.* Available from: http://www.cdt.org/wiretap/9706rpt.html/ [Accessed January 2005].

3. *Privacy and Human Rights: An International Survey of Privacy Laws and Practice (2003)*, published by Global Internet Liberty Campaign. Available from: http://www.gilc.org/privacy/survey/ [Accessed January 2005].

4. Long, Colin D. (1995) *Telecommunications Law and Practice.* Second Edition. Sweet & Maxwell, Australia.

5. *The New Encyclopedia Britannica.* (1994) Encyclopedia Britannica, Inc.