

CHAPTER 3

TECHNOLOGY SURVEILLANCE

Sajai Singh, Probir Roy Chowdhury, Amrut Joshi, and Govind Naidu
J. Sagar Associates
Bangalore, India

3.01 Introduction

To make a case for the regulation, and not abolition, of surveillance of individuals requires that surveillance in some form first be justified and then that safeguards be devised to limit its misuse.

The voluntaristic concepts of state formation, which most people know as the theories of social contract popularized by Hobbes, Locke, and Rousseau, conceive of the state as coming into existence by means of a contract among individuals to bring about regulation of their lives and order in society. The structural approach advocated by Marx and Engels theorized that the state emerged when better industrial techniques made possible the presence of different classes and that the states' function was to mediate the conflict between these classes by means of setting out laws and rules.

Other approaches to state formation, such as the ecological approach, believe that demographic expansion and the resultant pressures on resources provide the impetus for the formation of the state as a means of regulating access to and use of resources. More basic coercive models of state formation attribute the formation of the state to the need to expand and manage territories, although the examples used here are mostly ancient civilizations, like the Mayan and Aztec civilizations.

The common thread that runs through all of these approaches to state formation is the role of the state in governance and regulation by means of rules that people are required to follow. Having such a structure therefore requires that the population adhere to these rules for the system to work.

One way to achieve this is to rely on voluntary compliance by the population, and the other is to put in place a system of surveillance and retribution in order to punish violators of the rules laid down. Most, if not all, systems of governance have adopted the latter means of compliance and, therefore, states have a surveillance mechanism in place.

The limits of surveillance and the degree of intrusion into the private lives of individuals has been a topic of debate for years and has also featured prominently in literature for years, with authors like Aldous Huxley and, after him, George Orwell, conjuring up worlds regulated and monitored to an extreme. Most mythologies view the Gods as looking over humankind and intervening periodically to aid and protect it, a role many governments claim to be fulfilling today.

Anecdotal evidence from various texts and records illustrates the historicity of surveillance, and these cut across time and civilizations. The *Arthashastra*, by Kautilya, an Indian dating from approximately 300 B.C., places great emphasis on the role of knowledge gleaned from spies, both internally in a nation and outside it in maintaining a grip on power, echoes of which can be seen in Machiavelli's *Prince* written hundreds of years later. As long as surveillance has been a part of human life so probably has opposition to its excesses.

This chapter explores the ways by which laws of various jurisdictions seek to achieve the "correlation between adequate intelligence to guarantee our nation's security on the one hand, and the preservation of basic human rights on the other" that President Carter referred to. The next section looks at the technologies available to entities for undertaking surveillance.

This is followed by a section that looks at the rights of an entity conducting surveillance and the situations under which surveillance may be undertaken. The chapter then looks at the protections a subject of surveillance can invoke and then the procedure to be followed when surveillance is carried out. It must be kept in mind that the statutes and case law analyzed in this chapter are indicative in nature and are not exhaustive. They have been chosen to illustrate the principles states apply while dealing with the issue of surveillance.

3.02 Modes of Surveillance

(a) In General

In the 1960s, there were two identifiable forms of surveillance, i.e., physical and data,¹ the most basic form of surveillance is physical surveillance, which

1 Westin, *Privacy and Freedom* (1967).

comprises of watching and listening (visual and aural surveillance). However, with the constant evolution in technology, monitoring today may be undertaken remotely in space, with the aid of image amplification devices such as field glasses, infrared binoculars, light amplifiers, and satellite cameras, and sound-amplification devices, such as directional microphones.

Today, the boundaries have been blurred with the application of information technology linking surveillance techniques into a near seamless web of surveillance. Thus, it may be appropriate to categorize surveillance that is carried out with the assistance of technological devices as “technology-assisted surveillance”. Some of the common tools of “technology-assisted surveillance” are described below.

(b) Dataveillance

(i) In General

Apart from physical surveillance and technologically assisted surveillance, the other major form of surveillance is referred to as dataveillance. Dataveillance is the systematic use of personal data systems in the investigation or monitoring of the actions of communications of one or more persons. dataveillance could be further categorized into two major categories, i.e., personal dataveillance and mass dataveillance.

The distinction between personal and mass dataveillance is that the former is concerned with analyzing the information held on a particular individual or group (i.e., one which has already been singled out), while mass dataveillance is concerned with the examination of a wide range of subjects in an attempt to identify those who “fit” the search criteria (in other words, personal dataveillance is the end result of mass dataveillance).²

(ii) Credit Bureaus

Some of the major players in the information collection industry are the so-called “credit bureaus”. The largest three in the United States are Experian (formerly TRW Information Systems and Services), Equifax, and Trans Union.

In the United States, legal recourse for matters concerning credit bureaus can be sought through the Fair Credit Reporting Act of 1970, which requires that bureaus provide correct and complete information in credit reports. However, the legislation has been criticized on the grounds that anyone with a “legitimate business need” can obtain a credit report. The word legitimate is not defined in the Act.

² Clarke, *Information Technology and Dataveillance*, at <http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html>, visited on 2 September 2004.

(iii) Computer Matching and Profiling

While data matching and profiling are particular kinds of dataveillance techniques, they are not synonymous terms. Data matching refers to:

. . . exercises designed to assist in the detection of fraud are widely in operation in both the public and private sectors. The term “data matching” essentially means the comparison of data collected by different data users (or by the same data user in different contexts).

The aim of the comparison is not primarily the creation of a larger file of information about the data subject, but the identification of anomalies and inconsistencies within a single set of data or between two or more different sets.

Profiling, on the other hand, is a technique whereby a set of characteristics of a particular class of person is inferred from past experience, and data-holdings are searched for individuals with a close fit to that set of characteristics. An example of profiling is that of airline passenger profiling. Some mass dataveillance systems available in the United States are discussed below to illustrate the extent to which dataveillance can be conducted.

(iv) ECHELON

The United States National Security Agency has created a global spy system, code-named ECHELON, which captures and analyzes virtually every telephone call, telefax, email, and telex message sent anywhere in the world. ECHELON is controlled by the National Security Agency and is operated in conjunction with the Government Communications Headquarters (GCHQ) of England, the Communications Security Establishment (CSE) of Canada, the Australian Defense Security Directorate (DSD), and the General Communications Security Bureau (GCSB) of New Zealand. These organizations are bound together under a 1948 agreement, UKUSA.

ECHELON is designed primarily for non-military targets: governments, organizations, businesses, and individuals in virtually every country. It potentially affects every person communicating between (and sometimes within) countries anywhere in the world.

The backbone of the ECHELON network is the massive listening and reception stations directed at the Intelsat and Inmarsat satellites that are responsible for the vast majority of phone and fax communications traffic within and between countries and continents. The 20 Intelsat satellites follow a geo-stationary orbit locked onto a particular point on the Equator. These satellites carry primarily civilian traffic, but they do additionally carry diplomatic and governmental communications that are of particular interest to the UKUSA parties.

The extraordinary ability of ECHELON to intercept most of the communications traffic in the world is breathtaking in its scope. However, the power of ECHELON resides in its ability to decrypt, filter, examine, and codify messages into selective categories for further analysis by intelligence agents from the various UKUSA agencies. As the electronic signals are brought into the station, they are fed through the massive computer systems, where voice recognition, optical character recognition (OCR), and data information engines work on the messages.

(v) *Total Informational Awareness*

Total Informational Awareness is a project of the United States Department of Defense. Total Informational Awareness (TIA) is designed to gather personal data on a grand scale, including emails, telephone calls, financial records, transportation habits, and medical information.

Its proponents believe that, by scanning and analyzing this massive amount of data, government agents will be able to predict and prevent crime.

(vi) *Carnivore*

Carnivore is an Internet surveillance program, which is currently used by the United States government. It is somewhat similar to ECHELON. Contrary to prior assertions, a subsequent government-commissioned review panel found that Carnivore is indeed capable of collecting all communications over the segment of the network being watched.

Carnivore is being replaced by an even more powerful system, known as DCS 1000, or Enhanced Carnivore, which reportedly has higher capacity to deal with speedier broadband networks. The United States government also has issued a controversial field guidance memorandum regarding the installation and operation for this family of surveillance tools.

(vii) *Oasis and Fluent*

Oasis and Fluent are two programs which experts believe may be used to enhance ECHELON's capabilities. One of these, Oasis, automatically creates machine-readable transcripts from television and audio broadcasts. Reports indicate that Oasis can distinguish individual speakers and detect personal characteristics (such as gender) and denote these characteristics in the transcripts it creates.

The other program, FLUENT, allows English-language keyword searches of non-English materials. This data-mining tool not only finds pertinent documents, but also translates them, although the number of languages that can currently be translated is apparently limited (Russian, Chinese, Portuguese, Serbo-Croatian, Korean, and Ukrainian). In addition, FLUENT displays the

frequency with which a given word is used in a document and can handle alternate search term spellings.

(viii) *CALEA*

The United States Communications Assistance for Law Enforcement Act (CALEA) generally requires telecommunications carriers to modify their existing networks and to design and deploy new generations of equipment (including software), all to ensure that carriers can meet certain specified “capability” and “capacity” requirements related to the ability of authorized government agencies to engage in wiretapping.

3.03 Conditions for Surveillance

(a) United States

In the United States, the Foreign Intelligence Surveillance Act, 1978, was enacted for the purpose of regulating national security. The Foreign Intelligence and Surveillance Court that was constituted under the Foreign Intelligence Surveillance Act was set up primarily for dealing with cases relating to national security that have a foreign nexus and where the role of the surveyor is assumed by the state.

Under the Foreign Intelligence Surveillance Act, for an application for surveillance to be upheld, the state is required to show that the target of the investigation is a foreign power or agent of a foreign power and that the place to be monitored or searched is or will be used by the target.³ However, when the subject is a United States person, a higher probable cause standard is imposed and the application must show that “the acquisition of such information is necessary to national defense or security or the conduct of foreign affairs”.⁴

Therefore, as long as the application relates to a foreign power or agent of a foreign power, the test to be satisfied relates to the identity of the subject. In contrast, probable cause in a criminal investigation:

. . . exists where the facts and circumstances within their [the officers] knowledge . . . [are] sufficient in themselves to warrant a man of reasonable caution in the belief that an offence has been or is being committed.⁵

3 50 United States Code, section 1805(a).

4 National Security Agency Report to Congress: “Legal Standards for the Intelligence Community in Conducting Electronic Surveillance” (2001), available at <http://www.fas.org/irp/nsa/standards.html> (last visited 17 December 2002).

5 *Brinegar v. United States*, 338 U.S. 160, at pp. 175–76 (1949) (first and third alterations in original) (quoting *Carroll v. United States*, 267 U.S. 132, at p. 162) (1925)).

This test, which is the kind of standard most jurisdictions use for investigations, relates to a state of fact or events.

Courts have permitted evidence gathered in the Foreign Intelligence Surveillance Act investigations to be used in criminal convictions with the stipulation that foreign intelligence gathering be the “primary purpose” of the surveillance.⁶ The courts have found that evidence resulting from surveillance conducted under the Foreign Intelligence Surveillance Act warrant is not prohibited even if the government foresees that the results of such surveillance will later be used as evidence in a criminal trial.⁷

There is an exception to the warrant requirement in the Foreign Intelligence Surveillance Act process. If something illegal is in plain view, there is no need for a warrant because law enforcement officials did not need to search to find it. Originally, the exception required that police discover the evidence inadvertently.⁸ In *Horton v. California*,⁹ however, the Supreme Court eliminated the inadvertence requirement for a plain view seizure.

Another exception to the warrant requirement is the open fields’ doctrine. The doctrine suggests that if an item cannot be classified as a person, house, paper, or effect, the item is not entitled to Fourth Amendment protection against search or seizure.¹⁰ This is particularly true where the owner has not taken reasonable precautions to ensure privacy.

(b) United Kingdom

(i) In General

The United Kingdom has enacted several laws that lay down the grounds on which surveillance can be conducted. The following discussion deals with the various legislation and the requisites.

(ii) Data Protection Act, 1998

The Data Protection Act mostly covers workplace surveillance where the employer assumes the role of the surveyor. The Data Protection Act provides

6 *United States v. Megahay*, 553 F. Supp. 1180, at pp. 1189–1190 (E.D.N.Y., 1982).

7 *United States v. Pelton*, 835 F.2d 1067, at p. 1076 (4th Cir., 1987) (holding that “the Foreign Intelligence Surveillance Act surveillance is not tainted simply because the government can anticipate that the fruits of the surveillance may later be used . . . in a criminal trial”).

8 *Coolidge v. New Hampshire*, 403 U.S. 443, at pp. 469–471.

9 *Horton v. California*, 496 U.S. 128 (1990).

10 The Fourth, Amendment specifically discusses “the right of the people to be secure in their persons, houses, papers, and effects . . .”. United States Constitution, Amendment IV. However reasonable a landowner’s expectations of privacy may be, those expectations cannot convert a field into a “house” or an “effect”. *Oliver v. United States*, 466 U.S. 170, at p. 184 (1984) (White, J., *concurring*).

says that personal data that is processed for the purpose of preventing or detecting crime is exempt from the fair processing code and from the general obligation that the personal data be processed fairly. If an employer uses workplace surveillance for the purpose of detecting fraud, no notice is required to be given to workers about the data processing involved.

It provides that personal data may be obtained only for one or more specified and lawful purposes and may not be further processed in any manner incompatible with that purpose or those purposes. The principles of the Data Protection Act do not apply to the disclosure by a data controller of personal data processed for the purpose of preventing or detecting crime, to the extent that compliance with the principle would be likely to prejudice that purpose. Exemptions also are provided in the case of personal data whose disclosure is necessary for:

1. The purpose of, or in connection with, any legal proceedings (including prospective legal proceedings); or
2. The purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising, or defending legal rights, to the extent that the principle is inconsistent with the disclosure in question.

Thus, an employer may disclose to the police information gained through workplace surveillance that discloses criminal behavior, even where the possibility of such disclosure has not been previously notified to the worker.

Surveillance-related data whose processing was otherwise permitted by the Act would breach that provision if the data subject or other person who supplied it to the data controller was misled as to the purposes for which it was to be processed, save where the processing was in connection with the detection or prevention of a criminal offence or the apprehension or prosecution of an offender.

Furthermore, data processing will comply with the principles only where workers are provided with information as to the purpose or purposes for which the data is being processed. The only surveillance-related cases in which the obligation to process personal data fairly is likely not to apply is where the processing is “for the purpose of preventing or detecting crime” (as in a case in which surveillance is conducted to detect fraud).

The draft of the Code of Practice on Employment issued by the Information Commissioner (which deals with monitoring and surveillance) says that monitoring should occur only:

1. Where there is an identified business need;
2. Where its aims are not outweighed by its impact on staff;
3. To the extent that it is necessary; and

4. Save in exceptional cases, only with the full knowledge of staff concerned.

The Commissioner states that monitoring and surveillance should not go beyond that necessary to the aim pursued and that employers should strive to find alternative methods to achieve the ends pursued and suggests that covert monitoring can only be used where criminal behavior is suspected (and then only as narrowly as possible). The Data Protection Act, therefore, has the potential to curtail the ability of employers to lawfully engage in workplace-related surveillance.

(iii) Regulation of Investigatory Powers Act, 2000

The Regulation of Investigatory Powers Act was enacted to ensure that surveillance conducted by public authorities complies with the provisions of the Human Rights Act, 1998. To impose effective regulation on the interception of communications, section 1 makes it an offense:

. . . for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission¹¹

The new regime applies to both public postal and telecommunications systems and also to private telecommunications systems that are linked to a public network (such as business switchboards).¹² This interception offence is subject to two limitations.

Under section 1(3), if the interception is carried out without lawful authority under the Regulation of Investigatory Powers Act, then it will be actionable in civil law. However, by section 1(6), conduct is excluded from criminal liability if perpetrated or permitted by a person lawfully entitled to control the operation or the use of the system. Second, by section 1(5) the interception has lawful authority under the Regulation of Investigatory Powers Act if it falls within section 3, 4, or 5 (see text, below) or where an existing statutory power is used to obtain stored communications (such as a search under warrant or on arrest under powers in the Police and Criminal Evidence Act, 1984).

Section 3 authorizes certain kinds of interception where all parties to a communication have consented to the interception, or where the recipient consents and the communication is subject to surveillance under Part II of the

11 “Interception” and “transmission” of communications (but not postal items) are defined in section 2. “Communications” for these purposes do not include “traffic data”, since they are regulated by Part 1, Chapter 2. The territorial limitation of the Regulation of Investigatory Powers Act is explained by sections 2(4) and 20.

12 This responds to *Halford v. United Kingdom* (1997) 24 E.H.R.R. 523; *A v. France*, Ser A 277/B. It replaces a Home Office Circular 15/1999, Interception of Non-Public Telecommunications Networks (1999).

Regulation of Investigatory Powers Act. Section 4 provides for situations like complying with international agreements for mutual assistance¹³ and for certain cases where interception and recording is necessary for the carrying on of any business of monitoring or keeping a record.

More explicit lawful authority is provided for in the shape of interception warrants issued by the Home Secretary under section 5. The warrant issued must be “proportionate” to the purpose for which it is sought and it must be “necessary”.

(3) . . . a warrant is necessary on grounds falling within this subsection if it is necessary:

- (a) In the interests of national security;
- (b) For the purpose of preventing or detecting serious crime;
- (c) For the purpose of safeguarding the economic well-being of the United Kingdom; or
- (d) For the purpose, in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a warrant by virtue of paragraph (b), of giving effect to the provisions of any international mutual assistance agreement.

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

(c) European Union

In the European Union (EU), there are no specific statutes stating the grounds for surveillance. The European courts have laid down standard safeguards, which the surveying authority would have to keep in mind before conducting surveillance. The European Court of Justice adopts the approach that procedural standards should be complied with and, in a recent report,¹⁴ summarizes those as comprising:

1. Legality — The possibility of such interference must be clearly laid out in law, readily accessible, and precise so that citizens are aware of the circumstances under which surveillance may be undertaken or communications intercepted. It should go without saying that legality requires that the grounds for surveillance should be subject to prior judicial scrutiny.

13 For example, articles 12 and 13 of the Convention on Mutual Assistance in Criminal Matters between Member States of the European Union.

14 European Court of Justice, *Justice: Under Surveillance: Covert Policing and Human Rights Standards* (1998).

2. Necessity — The interference should be necessary because less intrusive means have been tried and failed or are inappropriate and the operation is likely to produce valuable material that would aid the investigation.
3. Proportionality — The intrusive measures should be proportional to the seriousness of the offence, bearing in mind the rights not only of the individual, but also those of others likely to be affected.
4. Accountability — There must be proper controls and adequate and effective remedies against abuse.

3.04 Protection Offered to a Subject of Surveillance

(a) United States

American scholars as far back as the 1800s have debated the existence of the right to privacy.¹⁵ The United States Supreme Court has found a limited “right to privacy” stemming from a combination of the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments.

The United States Constitution does not provide an explicit right to privacy, but it is implied in the Fourth Amendment. The Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. However, what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.

The Supreme Court, in *Keith*,¹⁶ noted that:

... there is, understandably, a deep-seated uneasiness and apprehension that electronic surveillance capability will be used to intrude on cherished privacy of law-abiding citizens.

The challenge for the court involved balancing the necessity of ensuring national security against the threat to individual liberties posed by unchecked executive surveillance authority.¹⁷

In weighing these competing interests, Justice Powell’s opinion expanded the principles that would guide all three branches of the federal government in the application of the Fourth Amendment to national security electronic surveillance.¹⁸ Powell noted that national security cases present a particularly

15 Warren and Brandeis, “The Right to Privacy”, 4 *Harv. L. Rev.* 193 (1890).

16 *United States v. United States District Court (Keith)*, 407 U.S. 297 (1972).

17 18 United States Code, section 2511(3).

18 *United States v. Duggan*, 743 F2d 59, at p. 72 (2d Cir., 1984) (noting that decision in *Keith* “made clear that the requirements of the Fourth Amendment may change” depending on governmental interests and that interests in national security context are “substantially different” from those in criminal investigations).

prickly situation because of the tremendous governmental interest and the likelihood of both unreasonable invasions of privacy and jeopardy to free speech rights.¹⁹

Although he recognized the vital importance of protecting the national security, Justice Powell's primary concern was ensuring the sanctity of political dissent — both public and private — in determining the application of the Fourth Amendment to national security surveillance.²⁰

For Powell, the Fourth Amendment had to serve as:

... an important working part of our machinery of government, operating . . . to check the "well-intentioned" but mistakenly over-zealous executive officers.

This constitutional function could not be guaranteed when domestic security surveillance was left entirely to the discretion of the executive:

Unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.

Thus, the court reiterated its assertion in *Katz* that some interposition of the judiciary between citizens and law enforcement must exist.²¹

It is clear that the United States provides to its citizens an implied right to privacy through the Constitution. The concept of the rational test basis would imply that a balance would have to be struck between the rights of the individual, on one hand, and societal needs, on the other.

19 *United States v. United States District Court (Keith)*, 407 U.S. 297 (1972), at p. 312 (noting that without national security, all constitutional liberties are at risk). See also at p. 313 ("National security cases, moreover, often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary" crime. Though the investigative duty of the executive may be stronger in such cases, so also is there a greater jeopardy to constitutionally protected speech").

20 *United States v. United States District Court (Keith)*, 407 U.S. 297 (1972), at p. 314 (discussing political dissent). Justice Powell noted: "The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse is essential to our free society".

21 *United States v. United States District Court (Keith)*, 407 U.S. 297 (1972), at p. 317 (noting that, while surveillance at issue may have been entirely reasonable, the court had never let this fact excuse lack of judicial involvement prior to surveillance); *id.* *United States v. United States District Court (Keith)*, 407 U.S. 297 (1972), at p. 318 (noting that judicially created exceptions to warrant requirement did not dilute principle of obtaining warrant prior to surveillance whenever practicable).

(b) Europe and the United Kingdom

The European Convention on Human Rights, 1950, addresses the issue of privacy as follows:

8(1). Everyone has the right to respect for his private and family life, his home, and his correspondence.

8(2). There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 8 of the European Convention on Human Rights provides a right to respect for private and family life, subject to the qualification in Article 8(2) that interference may occur where it is “in accordance with the law and is necessary in a democratic society in the interests of” the prevention of disorder or crime. The interrelationship between article 8(1) and (2) is not one of balancing the legitimate interference against the right;²² the article 8(2) qualifications clearly represent exceptions to article 8(1). The court determines whether surveillance interfered with privacy rights as broadly interpreted in article 8(1)²³ before assessing the article 8(2) elements in turn.

Article 13 provides that:

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

In the face of considerable opposition, this provision was not incorporated in the Human Rights Act.²⁴

In Convention terms, article 13 requires an “effective remedy” when there is a breach of article 8.²⁵ Logically, the effectiveness of the available remedy must lie in its ability to secure the protection offered by article 8 — in this context, a respect for privacy. The fact that the Human Rights Act does not incorporate article 13 does not negate domestic obligations to provide an

22 McHarg, “Reconciling Human Rights and the Public Interest: Conceptual Problems and Doctrinal Uncertainty in the Jurisprudence of the European Convention on Human Rights” (1999) 62 *M.L.R.* 671; Ashworth, “Serious Crime and Criminal Procedure”, *Human Rights* (2002).

23 *Kopp v. Switzerland* (1998) 27 *E.H.R.R.* 91; *Klass v. Germany* (1978) 2 *E.H.R.R.* 214.

24 Emmerson and Ashworth, *Human Rights and Criminal Justice* (2001), chapter 3.

25 Harris, O’Boyle, and Warbrick, *The Law of the European Convention on Human Rights* (1995), chapter 14.

effective remedy because the Convention must always be read as a whole,²⁶ and section 8 of the Human Rights Act provides a right to just and appropriate remedy.

In the United Kingdom, until the passage of the Human Rights Act, 1998, the concept of privacy was one that neither Parliament nor the courts had taken the initiative to develop.²⁷

In 1996, in *R v. Brown*,²⁸ Lord Hoffman stated that, “English common law does not know a general right of privacy and Parliament has been reluctant to enact one”. The House of Lords, later that year in a case concerning covert police surveillance, commented on the “continuing widespread concern at this apparent failure of the law”.²⁹ Such a reluctance to develop the law has partly been a result of the inherent difficulties in defining such a nebulous concept.

However, although “privacy” as a domestic legal term in England might be lacking clear parameters, the right to respect for private life under article 8 of the Convention brings with it decades of developing jurisprudence. The European Court’s jurisprudence lays down a minimum set of values that must be respected in signatory states, and, even prior to the Human Rights Act, this had impacted United Kingdom law and practice indirectly.³⁰

The Human Rights Act has brought about the development of a coherent and comprehensive system to ensure that all police action that might interfere with article 8 is convention compliant. It has also ensured that the courts must address directly the question of when a particular action interferes with the right to respect for private life.

A number of general principles have derived from the interpretation of the exceptions to the general right. First, if the primary right is engaged in a particular case, the restriction on that right must be “in accordance with the law”. European Convention jurisprudence has interpreted article 8(2) to mean that, regardless of the end to be achieved, no right guaranteed by the Convention should be interfered with unless a citizen knows the basis for the interference through an ascertainable national law.³¹ That law should be sufficiently clear

26 *Abdulaziz, Cabales, and Balkandali v. United Kingdom* (1985) 7 E.H.R.R. 471, at paragraph 60.

27 Feldman “Secrecy, Dignity, or Autonomy? Views of Privacy as a Civil Liberty” [1994] C.L.P. 41. Although, in recent years, the law of confidence had been developing: Fenwick and Phillipson, “The doctrine of confidence as a privacy remedy in the human rights era” [2000] 63 M.L.R. 660.

28 *R v. Brown* (1996) 1 All E.R. 545, at p. 556.

29 *R v. Khan* (1997) A.C. 558, at p. 582.

30 *R v. Secretary of State for the Home Department Ex p. Brind* [1991] 1 A.C. 696.

31 *Malone v. United Kingdom*. (1985) 7 E.H.R.R. 14; *Leander v. Sweden* (1987) 9 E.H.R.R. 433.

and accessible to ensure that people can adequately determine with some degree of certainty when and how their rights might be affected.

Second, any interference with the primary right must be directed towards a legitimate aim. In terms of the right to private life, restrictions that may be justified are found in article 8(2). The restrictions on the primary right are numerous and widely drawn, and it could be argued that it is not overly burdensome to require state conduct to remain within such boundaries. However, the list is intended to be exhaustive, and there should be no capacity for the state to add to those grounds.

In addition to being lawful, and for one of the prescribed purposes, the restriction also must be “necessary in a democratic society”. “Necessity”, although not defined in the Convention itself, has been interpreted by the European Court as not synonymous with “indispensable”, but not as flexible as “ordinary, useful, reasonable”, or “desirable”.³² Instead, what is required is that the interference with the primary right should be in response to “a pressing social need”.

The Human Rights Act has brought the concept of proportionality directly into play in the United Kingdom. In the context of qualified rights, such as article 8, proportionality has a special relevance. In *Brown v. Stott*,³³ Lord Steyn commented:

. . . a single-minded concentration on the pursuit of fundamental rights of individuals to the exclusion of the interests of the wider public might be subversive of the ideal of tolerant European liberal democracies. The fundamental rights of individuals are of supreme importance but those rights are not unlimited: we live in communities of individuals who also have rights.

Proportionality is a vital factor that attempts to find a balance between the interests of the individual and the interest of the wider community. Despite not explicitly appearing within the text of the Convention itself, it is said to be a defining characteristic of the way in which the courts seeks to protect human rights. It is, according to the Court, “inherent in the whole of the Convention”.³⁴

The jurisprudence of the European Court identifies numerous factors to be taken into account when considering the issue of proportionality.³⁵ For example, at the extreme, if a measure which restricts a right does so in such a way as to impair the very essence of the right, it will almost certainly be

32 *Silver v. United Kingdom* (1983) 5 E.H.R.R. 347, at paragraph 97.

33 *Brown v. Stott* [2001] 2 W.L.R. 817.

34 *Soering v. United Kingdom* (1989) 11 E.H.R.R. 439, at paragraph 89.

35 Starmer, *European Human Rights Law: The Human Rights Act 1998 and the European Convention on Human Rights* (1999), chapter 4.

disproportionate.³⁶ Furthermore, the need to have relevant and sufficient reasons provided in support of the particular measure has been emphasized:

The Court will look at the interference complained of in light of the case as a whole and determine whether the reasons adduced by the national authorities to justify it are relevant and sufficient and whether the means employed were proportionate to the legitimate aim pursued.

It also should be considered whether there is a less-restrictive alternative. It is unlikely that a measure could be considered to be proportionate where a less restrictive or intrusive alternative was available.

A balancing exercise takes place that requires a consideration of whether the interference with the right is greater than is necessary to achieve the aim.

This is not an exercise in balancing the right against the interference, but instead balances the nature and extent of the interference against the reasons for interfering.³⁷

A further factor in the proportionality equation is to assess the adequacy of procedural fairness in the decision-making process. Where a public body has exercised a discretion that restricts an individual's Convention rights, the rights of the affected individual should have been taken into account. For example, the policy should not be arbitrary but should be based on relevant considerations.³⁸ The guarantee against arbitrariness is one at the heart of the European Convention on Human Rights provisions. Proportionality can be more easily established where it could be shown that there are sufficient safeguards against abuse in place. This was expressed clearly in *Klass v. Germany*:

One of the fundamental principles of a democratic society is the rule of law . . . [which] implies, *inter alia*, that an interference by the executive authorities with an individual's rights should be subject to an effective control

Given that most policing actions will have a basis in law and will invariably satisfy the requirement of being in pursuit of a legitimate objective (principally, the prevention and detection of crime), the crux of a case will often be the proportionality of the action under scrutiny. In *Ex p. Kebilene*, Lord Hope commented:

. . . the Convention should be seen as an expression of fundamental principles rather than a set of mere rules. The questions which the

36 *Rees v. United Kingdom* (1987) 9 E.H.R.R. 56.

37 Feldman, *Civil Liberties and Human Rights in England and Wales* (2nd ed., 2002), at p. 57.

38 *W v. United Kingdom* (1988) 10 E.H.R.R. 29.

courts will have to decide in the application of these principles will involve questions of balance between competing interests and issues of proportionality.

The European Court has never sought to give a conclusive definition of privacy, considering it neither necessary nor desirable. However, in *Niemietz v. Germany*, the Court stated:

It would be too restrictive to limit the notion to an “inner circle” in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life also must comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of “private life” should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest opportunity of developing relationships with the outside world.

(c) India

In India, two main articles of the Constitution address privacy. These are the fundamental rights guaranteed by the Constitution to its citizens.

Article 21³⁹ gives protection of life and personal liberty. The Supreme Court has held that several un-enumerated rights fall within article 21, since the expression “personal liberty” is of the widest amplitude. This covers the right to privacy.⁴⁰ Wire-tapping of voluntary conversations, for the purpose of investigation of crime, has been upheld,⁴¹ assuming that privacy of conversation would be derived from “personal liberty”.

The judicial stand in India is that privacy is an inherent right guaranteed by the Constitution. There are certain safeguards that are provided in article 19(1)(d), read with article 21, to ensure that privacy rights are not violated and, until specific legislation is enacted in this regard, the judicial pronouncements will govern the field of the right to privacy.

39 Article 21 reads: “Protection of life and personal liberty. No person shall be deprived of his life or personal liberty except according to procedure established by law”.

40 *Gobind v. State of MP*, A.I.R. 1975 S.C. 1378 (paragraph 28); (1975) 2 S.C.C. 148. In this case, the petitioner was subjected to domiciliary visits by the police and was put under surveillance on the basis of criminal history.

41 *Malakani, RM v. State of Maharashtra*, A.I.R. 1973 S.C. 157, paragraph 30; (1973) 1 S.C.C. 471.

3.05 Procedures to Be Followed for Surveillance

(a) United States

In the mid-1970s, reports appeared in the American press alleging that the Central Intelligence Agency (CIA) had compiled files on thousands of American citizens. The reports led Congress to form investigative committees to consider the extent of executive surveillance abuses. The committees found that during the 1960s and 1970s, the CIA compiled a computerized database containing thousands of records chronicling the involvement of individual participants in the domestic antiwar movement. From these databases, the CIA:

. . . produced a steady stream of reports to the FBI and other agencies detailing the results of its various intelligence activities with respect to the antiwar movement.⁴²

The conclusion reached was that existing legal and policy constraints on intelligence activities were inadequate and that proper supervision and accountability within the Executive branch and to the Congress were sorely lacking. Although Title III provided a framework for criminal surveillance, the foreign intelligence exception was the creation of muddled judicial doctrine. Congress recognized that under the then-current system, action by the judiciary was purely remedial, and the courts essentially were powerless to prevent executive abuses before they occurred. Thus, Congress reacted to the executive's abuse of the foreign intelligence exception by creating a system in which "the judiciary would . . . be involved from the onset", effectively curbing the executive's ability to conduct warrantless national security surveillance that arguably contravened constitutional requirements.

The Foreign Intelligence Surveillance Act, 1978, was thus enacted. United States courts have permitted evidence gathered in the Foreign Intelligence Surveillance Act investigations to be used in criminal convictions with the stipulation that foreign intelligence gathering be the "primary

42 Reimers, notes: "Congressional involvement . . . remained minimal until the mid-1970s, [when] a series of especially troubling revelations appeared in the press concerning United States. Intelligence activities. Covert action programs involving assassination attempts against foreign leaders and covert efforts to effect changes in other governments were reported for the first time. The efforts of intelligence agencies to collect information concerning the political activities of United States citizens during the late 1960s and early 1970s were also documented extensively by the press". (quoting Select Committee on Intelligence, United States Senate, 103d Cong., 2nd Sess., Report on Legislative Oversight of Intelligence Activities: The United States Experience 3, at p. 4 (Comm. Print, 1994)).

purpose” of the surveillance.⁴³ The courts have found that evidence resulting from surveillance conducted under the Foreign Intelligence Surveillance Act warrant is not prohibited even if the government foresees that the results of such surveillance will later be used as evidence in a criminal trial.⁴⁴

In *Duggan*, the court acknowledged that surveillance in the interest of national security and criminal prosecution will often overlap, but that this intersection is mitigated by the requirement that foreign intelligence information gathering be the primary objective of the surveillance.⁴⁵ Courts have pointed out that the language of the Act itself, as well as the legislative history, indicates that evidence obtained through the Foreign Intelligence Surveillance Act surveillance was expected to be admissible in criminal proceedings.

The Foreign Intelligence Surveillance Act requires a showing of probable cause that an individual is linked to a foreign power or terrorist organization. It requires the preparation and presentation of a complete Foreign Intelligence Surveillance Act application to the Foreign Intelligence and Surveillance Court within 24 hours after the Attorney General’s authorization.⁴⁶

Neglecting to meet these time limit results is suppression of the information obtained during the surveillance or search. the Foreign Intelligence Surveillance Act is a complex statute outlining specific procedural requirements for conducting electronic surveillance. The Foreign Intelligence Surveillance Act restricts the use of electronic surveillance to monitoring “foreign powers” or their “agents” including “United States persons” to obtain “foreign intelligence information”.⁴⁷ After first obtaining the approval of the Attorney General, a federal official may apply for Foreign Intelligence Surveillance Act electronic surveillance warrant. The official must submit an application that includes:

1. The identity of the surveillance target;

43 *United States v. Megahey*, 533 F. Supp. 1180, at pp. 1189 and 1190 (E.D.N.Y., 1982).

44 *United States v. Pelton*, 835 F2d 1067, at p. 1076 (4th Cir., 1987) (holding that “the Foreign Intelligence Surveillance Act surveillance is not tainted simply because the government can anticipate that the fruits of the surveillance may later be used . . . in a criminal trial”).

45 *United States v. Duggan*, 743 F2d 59, at pp. 75–78 (2d Cir., 1984).

46 50 United States Code, sections 1805(e) and 1824(d) (1994).

47 Chiarella, “So Judge, How Do I Get That Foreign Intelligence Surveillance Act Warrant?: The Policy and Procedure for Conducting Electronic Surveillance”, *Army Law* (October 1997).

2. The information indicating that the target is a “foreign power”⁴⁸ or an “agent of a foreign power”;⁴⁹
3. Evidence that the location indicated for surveillance is being used or is about to be used by the foreign power or its agent; and
4. The type of surveillance, proposed minimization procedures, and certification that the information sought is “foreign intelligence information”.⁵⁰

48 50 United States Code, section 1801(a). “Foreign power” is defined as: (1) a foreign government or any component thereof, whether or not recognized by the United States; (2) a faction of a foreign nation or nations, not substantially composed of United States persons; (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; (4) a group engaged in international terrorism or activities in preparation therefor; (5) a foreign-based political organization, not substantially composed of United States persons; or (6) an entity that is directed and controlled by a foreign government or governments.

49 50 United States Code, section 1801(b). “Agent of a foreign power” is defined as: (1) any person other than a United States person, who - (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section; (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person’s presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or (2) any person who — (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States; (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States; (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, or on behalf of a foreign power; or (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

50 50 United States Code, section 1801(e). “Foreign intelligence information” is defined as: (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against — (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to — (A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States.

After the Foreign Intelligence Surveillance Act application has been approved by the appropriate federal agency, it is forwarded to the Office of Intelligence Policy Review at the Department of Justice.

The Office of Intelligence Policy Review assists the Attorney General and other senior Justice Department officials in fulfilling national security-related responsibilities. It provides legal advice and guidance to various elements of the United States Government that are engaged in national security-related activities. It oversees the implementation of the Foreign Intelligence Surveillance Act and other statutory, Executive Order, or Attorney General-based operational authorities for national security-related activities.⁵¹ The Office of Intelligence Policy Review conducts an independent review of the application to confirm that it contains all the required information. If the application is approved by the Office of Intelligence Policy Review, it is forwarded to the Foreign Intelligence and Surveillance Court.

The Foreign Intelligence and Surveillance Court performs an independent review of the Foreign Intelligence Surveillance Act application. Before issuing the order, the Foreign Intelligence and Surveillance Court determines whether there is “probable cause to believe that the target of the [electronic] surveillance is a foreign power or an agent of a foreign power”.⁵² In the case of a United States person, the determination must be that the target of the surveillance is not being considered “an agent of a foreign power solely on the basis of activities protected by the first amendment to the Constitution of the United States”.⁵³ The Foreign Intelligence and Surveillance Court also ascertains that the application includes requisite certification from the Department of Justice, indicating that the information sought is “foreign intelligence information” which cannot be obtained by other means.

The Foreign Intelligence and Surveillance Court consists of seven United States District Court judges drawn from different circuits, serving staggered, non-renewable, seven-year terms.⁵⁴ The Chief Justice of the United States chooses the Foreign Intelligence and Surveillance Court judges, who rotate their

51 United States Department of Justice, Office of Intelligence and Policy Review Organization, Mission and Functions Manual; see <http://www.usdoj.gov/jmd/mps/mission.htm> (last visited 26 November 2002).

52 *United States v. Pelton*, 835 F2d 1067, 1075 (4th Cir., 1987).

53 50 United States Code, section 1805(a)(3)(A).

54 Poole, “Inside America’s Secret Court: The Foreign Intelligence Surveillance Act”; see <http://fly.hiwaay.net/~pspoole/fiscshort.html> (last visited 8 September 2002) (describing the nature of the Foreign Intelligence and Surveillance Court proceedings).

duties in Washington, D.C. The judges carry out their duties in a “cipher-locked, windowless, secure room on the top floor of the Department of Justice”.⁵⁵

The Foreign Intelligence and Surveillance Court meets two days out of every month, with two of the judges routinely available on other days. The consideration of the Foreign Intelligence Surveillance Act applications is non adversarial and based solely on the presentation of the application through an Office of Intelligence Policy Review representative.⁵⁶

If an application is denied, it is immediately transmitted to a three-judge court of appeal, also composed of selected federal judges. If the appellate court affirms the Foreign Intelligence and Surveillance Court denial of a warrant, the government may apply for a writ of *certiorari* to the Supreme Court.⁵⁷

The Foreign Intelligence Surveillance Act’s secrecy also presents a unique problem for a criminal defendant seeking to suppress the Foreign Intelligence Surveillance Act’s surveillance evidence or challenge a conviction based on such evidence. Section 1806(f) of the Act requires that the district court judge entertaining a defendant’s challenge to a Foreign Intelligence Surveillance Act application “review *in camera* and *ex parte* the application, order, and such other [necessary] materials relating to the surveillance” whenever “the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States”.

Thus, the Foreign Intelligence Surveillance Act often will not allow a defendant the opportunity to contest adequately the validity of surveillance or the admissibility of crucial evidence obtained thereby. Although courts have affirmed the constitutionality of this reality, the provision nevertheless augments the possibility that governmental abuse of the Foreign Intelligence Surveillance Act will go undiscovered.⁵⁸

The definition of “foreign intelligence information” contained in the Foreign Intelligence Surveillance Act includes “sabotage or international terrorism

55 Foreign Intelligence Surveillance Act: Oversight Hearings Before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the House Committee on the Judiciary, 98th Cong. 2, at p. 5 (1983) (statement of Mary C. Lawton, Counsel for Intelligence Policy).

56 Robinson, “We’re Listening! Electronic Eavesdropping, the Foreign Intelligence Surveillance Act, and the Secret Court”, 36 *Willamette L. Rev.* 51, at p. 65 (2000).

57 Birkenstock, “The Foreign Intelligence Surveillance Act and Standards of Probable Cause: An Alternative Analysis”, 80 *Geo. L.J.* 843, at p. 848 (1992).

58 *United States v. Belfield*, 692 F2d 141, at pp. 148 and 149 (D.C. Cir., 1982) (finding that 50 United States Code, section 1806(f), does not violate the Fifth and Sixth Amendments).

by a foreign power or an agent of a foreign power”. The definition of an “agent of a foreign power” includes any person who “knowingly engages in clandestine intelligence gathering activities . . . which involve or may involve a violation of the criminal statutes of the United States”, or “knowingly engages in sabotage or international terrorism”.

“International terrorism” means activities that involve violent acts or acts dangerous to human life and that are a violation of the criminal laws of the United States or of any State. The first thing that should be apparent is the breadth of these definitions. “Agent of a foreign power” is defined in behavioral terms, as one engaged in activities which “involve or may involve a violation of the criminal statutes of the United States”, or as one who engages in international terrorism. The definition of “international terrorism” has now been expanded to encompass any violent act that would violate the criminal laws of the United States or of any state.

The Foreign Intelligence and Surveillance Court carefully detailed these definitions in showing how the Foreign Intelligence Surveillance Act permits the investigation of criminal behavior. The terms used above include definitions of criminal behavior so broad as to encompass any violation of the criminal statutes of the United States, and any violent act which would violate the criminal law of the United States or any state. It is this broad definition of criminal behavior which the Foreign Intelligence and Surveillance Court says can now provide the purpose behind the Foreign Intelligence Surveillance Act surveillance.

In effect, the exception permitting investigation of some criminal activity swallows the rule that foreign intelligence information should be the primary purpose behind the surveillance. This reasoning permits surveillance not governed by the dictates of the Fourth Amendment to be used to conduct investigations which are primarily criminal so long as the Attorney General informs the Foreign Intelligence and Surveillance Court that “a significant purpose” behind the surveillance also is foreign intelligence. The court’s ruling not only offends the Fourth Amendment, but it is a tragically bad policy.⁵⁹

The Uniting and Strengthening of America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (United States Patriot Act) was enacted on 26 October 2001, less than two months after the terrorist attacks. In a press release, a member of the United States Congress commended the passage of the Act, indicating:

The Patriot Act modernizes wiretapping laws to keep up with changing technologies such as cell phones, voice mail and e-mail. Current wiretapping laws are outdated. In today’s technologically advanced society,

59 50 United States Code, section 1801(e)(1)(B) and 1801(b)(2)(A) and (C).

people communicate through a variety of means By allowing “roving surveillance” of suspected terrorists, law enforcement officials will be able to more effectively monitor their communications and intercept terrorist activity.⁶⁰

The United States Patriot Act expands the Foreign Intelligence Surveillance Act to allow “roving” surveillance, enabling government investigators to intercept all of a suspect’s wire or electronic communications relating to the conduct under investigation, regardless of the suspect’s location when communicating. This modification was necessary to address the evolution of modern technology. Such roving wiretaps enable surveillance of a person’s conversations on a cellular phone or of a target that moves from phone to phone.

The United States Patriot Act extends the roving wiretap authority to intelligence wiretaps.⁶¹ This authorization has the potential to extend nationwide.

The United States Patriot Act expands the government’s ability to obtain a court order under the Foreign Intelligence Surveillance Act for pen register or trap and trace surveillance. This eliminates the requirement that the government certify that it has reason to believe that the surveillance is being conducted on a line or device that is or was used in “communications with” someone involved in international terrorism or intelligence activities that may violate United States criminal law or a foreign power or its agent whose communication is believed to concern terrorism or intelligence activities that violate United States law.⁶²

This requirement is replaced with the requirement that the government certify that the information sought is “relevant to an ongoing criminal investigation”. If the government makes such a showing, a judge “must” grant the order. There is a limitation placed on this expanded provision, stating that a Foreign Intelligence Surveillance Act court order should not authorize the gathering of foreign intelligence information for an investigation concerning surveillance of a United States person when the person has been singled out for investigation “solely on the basis of” First Amendment activities.⁶³

These changes are a significant alteration to the mechanics of the Foreign Intelligence Surveillance Act because the language of the United States Patriot Act appears to obviate judicial discretion. The judge “must” grant the order, a

60 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (United States Patriot Act) Act of 2001, Pub. L. Number 107-56, 115 Stat. 272 (2001).

61 United States Patriot Act, section 206.

62 United States Patriot Act, section 214(a)(4) (amending 50 United States Code, section 1842(c)(3)).

63 United States Patriot Act, section 214 (amending 50 United States Code, section 1842(d)(2)(A)).

phrase that seems to mandate judicial issuance of a Foreign Intelligence Surveillance Act warrant.⁶⁴ Changes to the provisions for trap and trace would also permit a much broader collection of information than previously permitted under the Foreign Intelligence Surveillance Act. The Federal Bureau of Investigation (FBI) could collect not only the e-mail address of a communication, but also the subject header and information about URLs accessed, revealing information such as search queries, Web sites viewed, and online purchases.

(b) United Kingdom

(i) In General

Legislation was passed permitting a broad range of surveillance activity in the United Kingdom, promising to protect human rights and act as a check on the government's surveillance powers, i.e., the Regulation of Investigatory Powers Act, 2000. The Regulation of Investigatory Powers Act and the Terrorism Act, 2000, are permanent pieces of legislation, granting broad investigatory powers to the government, whose existence is not contingent on a state of emergency.

The United Kingdom government responded to the September 11 attacks by aggressively using these powers and justifying their expansion and solidification.⁶⁵

(ii) Regulation of Investigatory Powers Act, 2000

The Regulation of Investigatory Powers Act was enacted to ensure that certain surveillance activities, conducted by public authorities, complied with the Human Rights Act 1998. The Act signals both the importance of forms of surveillance as techniques of policing and the human rights apprehensions which those strategies engender.

The Regulation of Investigatory Powers Act regulates various privacy invasive activities through a system of authorizations and warrants. The authorizations or warrants can only be granted when the investigatory activity is necessary for one of the statutorily prescribed purposes and is a proportionate means of achieving that purpose. This system is designed to ensure that any interference with article 8(1) of the European Convention on Human Right right can be justified as necessary limitations on the right.

64 Strickland, "Information and the War against Terrorism, Part III: New Information-Related Laws and the Impact on Civil Liberties", *Bull. Am. Soc'y for Info. Sci.*, (February–March, 2002), at p. 23.

65 Amnesty International, United Kingdom: "Rights Denied: the UK's Response to 11 September 2001"; see <http://www.statewatch.org>.

Interception of communications may be authorized by an interception warrant, issued by the Secretary of State. Such a warrant can only be issued if the Secretary of State believes that the interception is necessary in the interests of national security, for the purpose of detecting or preventing serious crime or for the purpose of safeguarding the economic well-being of the United Kingdom.⁶⁶ In addition, the Secretary of State must believe that the conduct authorized by the warrant is proportionate to the objective of the interception, which includes consideration of alternative means of achieving the objective.⁶⁷

At a theoretical level, these limits on the issuance of warrants comply fully with article 8(2) of the European Convention on Human Rights' necessity requirements. However, as discussed below, theoretical compliance is no guarantee of practical compliance in the absence of an effective supervisory system.

Authorization for access to communications data follows the necessity and proportionality approach taken in relation to interception warrants. However, there are two significant points of difference. First, authorization may be an internal process and does not require the approval of the Secretary of State.⁶⁸ Second, access may be authorized on substantially wider grounds than those applicable to interceptions. The permissible grounds include:

1. The interests of national security and the prevention or detection of crime or disorder;
2. The economic well-being of the United Kingdom;
3. The interests of public safety;
4. The protection of public health;
5. The assessment or collection of tax, duty, levy, or other governmental charge;
6. In an emergency, entailing threat of death or injury, or damage to a person's health; or
7. Any other purpose specified by the Secretary of State by order.⁶⁹

It is doubtful whether the assessment or collection of governmental charges falls within the legitimate aims. Furthermore, the provision for "any other

⁶⁶ Regulation of Investigatory Powers Act, section 5(2) and (3).

⁶⁷ Regulation of Investigatory Powers Act, section 5(2)(b) and (4).

⁶⁸ Regulation of Investigatory Powers Act, section 22. The European Court of Human Rights criticized internal authorization in *Kopp v. Switzerland* (1998) 27 E.H.R.R. 91, indicating that such a practice is inconsistent with the rule of law.

⁶⁹ Regulation of Investigatory Powers Act, section 22(2).

purpose” to be specified by the Secretary of State is inconsistent with the tightly prescriptive nature of article 8.

Directed surveillance and the use of covert human intelligence sources may be authorized on a similar basis as access to communications data. While the list of permissible purposes is slightly narrower, the problematic purposes, identified above, are both present. By contrast, the bases of authorization for intrusive surveillance are significantly more limited. Authorization can only be granted in the interests of national security, for the prevention or detection of serious crime or in the interests of the economic well-being of the United Kingdom.

Authorization also can be granted where the authorized activity is proportionate to what it seeks to achieve. Only the Secretary of State has the authority to prohibit certain conduct or impose additional requirements for authorization on certain types of directed surveillance.

The Regulation of Investigatory Powers Act provides for independent scrutiny of the investigatory powers through the appointment of various Commissioners. The Interception of Communications Commissioner has responsibility for reviewing the granting and exercise of interception warrants, as well as monitoring access to communications data and investigations involving encrypted data.⁷⁰ Covert surveillance is, in the main part, the responsibility of the Chief and Assistant Surveillance Commissioners.⁷¹

Finally, the Intelligence Services Commissioner reviews the authorization and exercise of covert surveillance activities and investigations into encrypted data undertaken by the intelligence services, Ministry of Defense, and armed forces, in places other than Northern Ireland.⁷²

The supervision and monitoring provided by the Commissioners is the central privacy safeguard in the Regulation of Investigatory Powers Act system. In practical terms, it is of more importance than the Investigatory Powers Tribunal since the value of a complaints-based system of scrutiny is undermined by the inherent secrecy of covert investigatory activities. Unfortunately, this key supervisory and accountability mechanism has serious deficiencies.

Its major failing is the absence of independent judicial authorization of activities. The role of the Commissioners is limited to retrospective review of the exercise of the Regulation of Investigatory Powers Act powers. The only exception to this position involves intrusive surveillance authorizations, which are subject to approval by a Surveillance Commissioner, except in

70 Regulation of Investigatory Powers Act, section 57.

71 Regulation of Investigatory Powers Act, sections 62 and 63.

72 Regulation of Investigatory Powers Act, section 59. The Investigatory Powers Commissioner for Northern Ireland, provided for in section 61, has monitoring responsibility for Northern Ireland.

cases of urgency.⁷³ Retrospective review is likely to be less rigorous than prior scrutiny, and it may well be easier to satisfy the requirements of necessity and proportionality when armed with the incriminating results of the surveillance. This creates the risk that although the statutory authorization regime may comply with article 8, individual exercises of the investigatory powers could be unnecessary or disproportionate.

A further concern is that not all authorizations are subject to scrutiny; only those selected at random by the Commissioner will be reviewed. Accordingly, a substantial number of authorizations may never be subject to any form of independent scrutiny. This prospect is particularly alarming when regard is had to the significant number of errors reported by the Commissioners. For example, in his 2001 Report, the Interception Commissioner stated that there had been 43 errors and that he remained “concerned about the number of errors reported during the year”.⁷⁴

In addition to functional deficiencies, it is questionable whether the Commissioners have the time and resources necessary to provide effective oversight. Both the Chief Surveillance and Interception Commissioners in their annual reports have identified staffing shortages as major problems.⁷⁵ Although the situation has improved as a result of staff increases, shortages are likely to reoccur with the substantial increase in duties that will occur when further provisions of the Regulation of Investigatory Powers Act enter into force. The limits on the ability of the Commissioners to provide rigorous review is reflected in the comment of the Chief Surveillance Commissioner that:

I am hopeful that . . . I shall be able to keep under review, as amply as Parliament must be taken to expect of me, the exercise and performance of the surveillance powers and duties.⁷⁶

Complementing the appointment of Commissioners, Part IV of the Regulation of Investigatory Powers Act establishes the Investigatory Powers Tribunal as a means of receiving complaints and providing redress. The Tribunal’s key functions are to address complaints, under section 7(1)(a) of the Human Rights Act, against the intelligence services and in relation to the exercise of powers under the Regulation of Investigatory Powers Act.⁷⁷

While its jurisdiction may be comprehensive, its efficacy as a check and balance on those exercising investigatory powers is limited by a number of

73 Regulation of Investigatory Powers Act, section 36.

74 Report of the Interception of Communications Commissioner for 2001 (2002 H.C. 1243), at paragraphs 11 and 67.

75 Report of the Interception of Communications Commissioner for 2000, Cm. 5296 (2001), at paragraph 20.

76 Home Office Briefing (January 2002).

77 Regulation of Investigatory Powers Act, section 65.

factors. First, the absence of any disclosure obligation means that the majority of interference with privacy will be undetected.⁷⁸ In most cases, an individual will only discover that he or she has been the subject of interception or surveillance if criminal proceedings ensue. Secondly, the secrecy surrounding Tribunal proceedings impedes the ability of complainants to present an effective case. Finally, the lack of any appeal process denies an opportunity for potential deficiencies in the initial hearing to be remedied at a later stage.⁷⁹

Applicants have challenged the secretive nature of Tribunal proceedings. In a recent decision on that challenge, the Tribunal quashed a rule made by the Home Secretary which obliged the Tribunal to conduct all proceedings in private, irrespective of the circumstances.⁸⁰

It creates the possibility that, in the future, the Tribunal will hear certain elements of proceedings in public and that complainants, as well as their legal representatives, will be able to attend parts of the hearing. However, it is likely that this transparency will extend only to the procedural aspects of proceedings and that the substantive content will remain secret. Indeed, the decision does not alter the position that complainants cannot be informed of arguments made or see evidence adduced by a public authority where to do so would entail a risk to national security, even when that information is critical to the case.

Under section 71 of the Regulation of Investigatory Powers Act, the Secretary of State is required to issue one or more Codes of Practice relating to the exercise of the investigatory powers and duties. These Codes are designed to provide guidance to the public authorities affected by the Act and may serve as a guide to good practice. A number of Codes of Practice have been the subject of public consultation, and three have entered into force.⁸¹

The Codes currently in force contain additional safeguards which may assist in limiting arbitrary interference with privacy. All three Codes stipulate that particular care should be taken in cases where the affected individual might reasonably expect a high degree of privacy or where confidential information is involved.⁸²

78 The Tribunal received only 102 new applications between 2 October 2000 and 31 December 2001.

79 Regulation of Investigatory Powers Act, section 67(8).

80 This decision was described by the Tribunal itself as “the most significant case ever to come before the Tribunal”.

81 The Covert Surveillance Code of Practice, Interception of Communications Code of Practice, and Covert Human Intelligence Sources Code of Practice have entered into force. There has also been consultation on the Draft Access to Communications Data Code of Practice.

82 Part 3 of both the Covert Surveillance Code of Practice and the Covert Human Intelligence Sources Code of Practice and paragraph 3.2 of the Interception of Communications Code of Practice.

In addition, a number of safeguards are set out in relation to communications subject to legal privilege.⁸³ However, as the Codes have no binding force and there are no consequences for their disregard, the value of these safeguards is limited.

(iii) Police Act

Part III of the Police Act, 1997, establishes a system to authorize various methods of covert surveillance. Its great weakness is that the scheme does not require mandatory judicial supervision.⁸⁴ There are, however, many constraints:

1. Authorization will normally be given by the chief officer of the force and not by lower ranks;
2. The criteria for interference with property are reasonably specific;
3. All authorizations will be scrutinized by the commissioners; and
4. There are channels for complaint.

The key criteria for authorizations are laid down in section 93(2) of the Police Act. The authorization should only be given where the authorizing officer believes that:

1. The action is necessary as it will be of “substantial value” in the prevention or detection of “serious crime”;⁸⁵
2. The objectives of the action cannot reasonably be achieved by other means; and
3. The action should be proportional, i.e., the extent of the intrusion should be commensurate with the seriousness of the offence.

(c) European Union

As discussed above, European courts have adopted the approach that procedural standards should be complied, which include:

1. Legality;
2. Necessity;
3. Proportionality; and
4. Accountability.

83 Paragraphs 3.3–3.9 of both the Covert Surveillance Code of Practice and the Covert Human Intelligence Sources Code of Practice and paragraphs 3.3-3.8 of the Interception of Communications Code of Practice.

84 Prior judicial authorization is the norm in Australia, New Zealand, the United States, Canada, France, and The Netherlands before there can be lawful interception of communications.

85 Police Act, section 93(4).

In *Klass v. Germany*, the court provided the following general guidance as to the legislation authorizing surveillance:

1. The legislation must be designed to ensure that surveillance is not ordered haphazardly, irregularly, or without due and proper care;
2. Surveillance must be reviewed and must be accompanied by procedures which guarantee individual rights;
3. It is, in principle, desirable to entrust the supervisory control to a judge in accordance with the rule of law, but other safeguards might suffice if they are independent and vested with sufficient powers to exercise an effective and continuous control; and
4. If the surveillance is justified under article 8(2) of the European Convention on Human Rights, the failure to inform the individual under surveillance of this fact afterwards is, in principle, justified.

(d) Canada

In Canada, there are certain prescribed guidelines for surveillance conducted by employers. To minimize the negative effects of searching and monitoring employees while effectively protecting legitimate employer interests, all employers (unionized or not) are well-advised to adhere to the legal principles established by Canadian labor arbitrators. Employers must balance their needs against employees' privacy interests and ensure that the search and surveillance methods they use are commensurate with their legitimate business interests.

For example, limiting surveillance to determining the time, origin, destination, and length of an e-mail transmission will allow an employer to determine if the communication was for business or personal purposes. By restricting monitoring in this way, employers can protect their interests without accessing the content of personal communications. With respect to the Internet, the types of websites visited by an employee will indicate whether an employee is using the Internet for personal or business use and whether the employee is accessing illegal or inappropriate material.

Furthermore, employers should establish policies regarding proper monitoring procedures for e-mail, Internet, and telephone usage. The policies should make clear to employees the scope and intent of the monitoring, including:

1. The purpose of the monitoring;
2. The extent to which monitoring will be conducted;
3. The fact that telephones, voice mail, e-mail, and the Internet are to be used for business purposes only;

4. The basis on business use will be distinguished from personal use;
5. The means for accomplishing monitoring and its proposed frequency; and
6. A clear demarcation between what is considered to be a public versus a private communication.⁸⁶

Monitoring policies also should emphasize that employees have a reduced expectation of privacy in the workplace. If possible, such policies should be made part of the terms and conditions of employment at the time of hire. Employers should also consider seeking signed acknowledgements from employees indicating that they understand the policy and consent to monitoring consistent with the policy.

Monitoring employees' use of e-mail, the Internet can be done from a technical point of view. It may be done legally in many circumstances. Employers certainly have a legitimate interest in ensuring that their resources are used in an appropriate manner and that their workplaces are secure.

Nonetheless, it is not self-evident that employers should monitor employees to the full extent of their ability to do so since the corresponding erosion of employee privacy also may have negative effects on the workplace to the employer's ultimate detriment.

In the final analysis, employers must keep in mind that positive employee relations are fundamental to maintaining a productive workplace, and that this interest should be at the heart of any decision to conduct searches or surveillance of employees.

(e) India

The Indian Constitution guarantees to all its citizens, under article 21, the right to life and personal liberty.

The legal framework in India does provide for protection for privacy of individuals. If such fundamentals are already imbedded into the basic framework, it would not be difficult to frame rules or regulations that could govern surveillance procedures and at the same time afford protection to the citizens from indiscriminate intrusions.

In *People's Union of Civil Liberties v. Union of India and Another*,⁸⁷ the Supreme Court of India laid down the following guidelines for interception

86 Sherrard, "Workplace Searches and Surveillance versus the Employee's Right to Privacy", 48 *U.N.B. L.J.* 283.

87 *People's Union of Civil Liberties v. Union of India and Another*, W.P. (C). Number 256/1991.

of telephonic conversations; it does not address the issue of surveillance *per se*, but is a forerunner for regulations to be framed. The Supreme Court held:

1. An order for telephone-tapping in terms of section 5(2) of the Act may not be issued except by the Home Secretary, Government of India (Central Government) and Home Secretaries of the State Governments. In an urgent case, the power may be delegated to an officer of the Home Department of the Government of India and the State Government not below the rank of Joint Secretary. A copy of the order must be sent to the Review Committee concerned within one week of the passing of the order.
2. The order must require the person to whom it is addressed to intercept in the course of his transmission, by means of the public telecommunication system, such communications as are described in the order. The order also may require the person to whom it is addressed to disclose the intercepted material to such person and in such manner as is described in the order.
3. The matters to be taken into account in considering whether an order is necessary under section 5(2) of the Act must include whether the information that is considered necessary to acquire could reasonably be acquired by other means.
4. The interception required under section 5(2) of the Act must be the interception of such communications as are sent to or from one or more addresses, specified in the order, being an address or addresses likely to be used for the transmission of communications to or from, one particular person specified or described in the order or one particular set of premises specified or described in the order.
5. The order under section 5(2) of the Act must, unless renewed, cease to have effect at the end of the period of two months from the date of issue. The authority which issued the order may, at any time before the end of the two months' period, renew the order if it considers that it is necessary to continue the order in terms of section 5(2) of the Act. The total period for the operation of the order may not exceed six months.
6. The authority that issued the order must maintain the following records: (a) the intercepted communications, (b) the extent to which the material is disclosed, (c) the number of persons and their identity to whom any of the material is disclosed, (d) the extent to which the material is copied, and (e) the number of copies made of any of the material.
7. The use of the intercepted material must be limited to the minimum that is necessary in terms of section 5(2) of the Act.

8. Each copy made of any of the intercepted material must be destroyed as soon as its retention is no longer necessary in terms of section 5(2) of the Act.
9. There must be a Review Committee consisting of the Cabinet Secretary, the Law Secretary and the Secretary, Telecommunication, at the level of the Central Government, The Review Committee at the State level shall consist of the Chief Secretary, Law Secretary, and another member other than the Home Secretary, appointed by the State Government.

The Committee must, on its own and within two months of the passing of the order by the authority concerned, investigate whether there is or has been a relevant order under section 5(2) of the Act. Where there is or has been an order, it must be determined whether there has been any contravention of the provisions of section 5(2) of the Act.

If, on an investigation, the Committee concludes that there has been a contravention of the provisions of section 5(2) of the Act, it must set aside the order under scrutiny of the Committee. It must further direct the destruction of the copies of the intercepted material.

If, on investigation, the Committee comes to the conclusion that there has been no contravention of the provisions of section 5(2) of the Act, it must record the finding to that effect.

The provisions in India relating to technology-assisted surveillance have not yet been framed, and the above provides the only safeguards in India against interception of telephonic conversations. There may not be a concrete system in place, but there are insights as to what could be a proposed regulatory authority.

Although there is an Information Technology Act 2000 (“Act”) in India, the Act does not cover provisions of surveillance and only covers the unauthorized use of information technology for hacking purposes and viewing unauthorized websites.

3.06 Conclusion

As indicated above, technology is making it increasingly possible to develop physically non-intrusive techniques of surveillance. The use of satellites and other remote monitoring tools have lessened the need to physically intrude on a person’s privacy.

This kind of technology has been both praised and pilloried — praised for enabling states to monitor data more effectively and so provide better security to their citizens and pilloried for enabling the state to intrude into what used to be private spaces and conversations. Therefore, technology cuts both

ways, and jurisprudence needs to keep up with these changes to ensure that the use of technology does not spread unchecked.

This is especially necessary in the light of the spread of global terrorism and the increased activity on the part of states to limit and control it. Moving to an extreme position in the name of national security could be a fallout, and legislatures and courts need to be wary of this possibility. Having looked at the statutes that govern the use of surveillance for the purposes of national security, one can see that they do not impose a very high threshold for surveillance. This is probably due to the nature of the subject they deal with, where governments would rather err on the side of caution and indulge in more, rather than less, surveillance so that the security of the country is not compromised. In contrast, statutes and case law that deal with surveillance of employees by their employers have higher thresholds since the concern being addressed there is not as critical as national security.

Given the nature of national security requirements, it may not be possible to put in place a detailed pre-surveillance approval procedure since speed is of the essence in such cases, but the surveillance authority should at least be able to make out a *prima facie* case for surveillance to some approving authority. An example of this process is the process in place under the Foreign Intelligence Surveillance Act in the United States where judges, who are not part of the same administrative set-up as the investigators, decide the validity of the applications made to them.

This system seems preferable to that under the Regulation of Investigatory Powers Act in the United Kingdom, where the approval for interception of and access to information is internal to the department and therefore possibly much more likely to be granted. The Foreign Intelligence Surveillance Act thus has a clearer system of checks and balances in place at the stage of starting surveillance.

In areas other than national security, for example, cases of other criminal laws, such a system also must be put in place so that the authority that wants to undertake surveillance does not become the authority that takes a decision on whether the surveillance is permissible or not. What needs to be ensured is that decisions on validity or otherwise are taken expeditiously so that the nothing gets delayed.

Cases such as employee surveillance, where the urgency of the matter is less, or the investigation of business-related offences, like those under the Enterprise Act of the United Kingdom, can undergo a slightly more rigorous process of pre-surveillance scrutiny because time need not be of the essence in these cases.

Once the decision to undertake surveillance is taken and the investigative authorities have begun the process, one must ensure that the process of

surveillance does not overstep the limits set out for it. If the investigation yields results and reaches the stage of prosecution in any case, the judge will examine the means by which the evidence was obtained, but even cases where no prosecution results need to be examined to prevent misuse of the surveillance procedures.

Periodic reporting requirements to the authority that sanctioned the surveillance could be put in place so that the sanctioning authority is aware of whether the original premise under which the sanction was granted was correct or not. Again, since this is prior to the subject of surveillance being informed, this also would be non-adversarial and would rely on a *prima facie* case being made out rather than clear-cut evidence being unearthed.

This kind of a procedure of periodic checks may actually be helpful for the rate of conviction in some countries because if the investigators need to report periodically, their method of investigation will be such as to satisfy the tests laid down in law and may run a much lower risk in court later of being rejected as having been done in violation of law.

In the event a person finds out he is the subject of surveillance, he needs to have recourse to the courts of law if the surveillance is intruding on his privacy. To this end, concepts of privacy have been developed in most jurisdictions which lay down the boundaries within which the state, or any other entity, cannot enter without the consent of the individual but which recognize that sometimes access to private information is necessitated by reasons of public safety and crime prevention. In cases where the intrusion is deemed necessary by the investigator, the court process forces the investigator to make the case for intrusion and assure that it satisfies the tests laid down in law for the intrusion.

If the case is made out, the subject will be obliged to go along with the investigation and, if not, the investigation must cease. The problem a subject of surveillance faces is that, other than physical surveillance, for example, where a person is being shadowed or a house is searched, it is very hard to establish covert and remote surveillance because the surveillance is not physically intrusive and because all the records of such surveillance are normally secret and inaccessible and, even in a court proceeding, the subject of surveillance may not be able to get full access to the surveillance documents and methodology.

This problem of granting access to surveillance documents is not one that can be solved easily, and there will always be proponents of granting no access in the name of security and of granting full access in the name of greater liberty and openness. A possible compromise between these two ends is the strengthening of the scrutinizing process that the investigators are subject to.

In the event the investigation is subject to a meaningful and independent scrutiny and periodic evaluation, the credibility of the investigation is enhanced and concerns of individuals will be addressed to some extent. While there may not be any means to completely eliminate the possibility of misuse of surveillance, it is possible thus to minimize it to some extent. It must be kept in mind that this process of scrutiny must be in addition to, and not a replacement for, the present procedural safeguards that have been built into surveillance procedures, as they exist today.

