CHAPTER-V
CHAPTER-V

DEVELOPMENT OF PRIVACY LAW: COMPARATIVE INTERNATIONAL PERSPECTIVE

5.1 An Overview

5.2 United States

5.3 United Kingdom

5.4 Australia

5.5 Canada

5.6 Ireland

5.7 Germany

5.8 Recapitulation
5.1 An Overview

There is an exciting global trend towards recognition of the right to privacy by States, Intergovernmental Organizations, Civil society and the People. There is a growing body of authoritative statement supporting the right to privacy. The United States seems to have been the first country to focus on privacy as a public issue. As early as the 1960’s American’s anxiety over creation and use of files on consumer’s credit triggered demand for public action. The ultimate result was federal legislation on credit records based on principles that became widely applied in other domains. One key result was America’s Privacy Act of 1974, governing administrative records held by federal agencies.

In 1973, Sweden passed its Data Protection Act, the first National Privacy Act in the world. By the end of 1970s, Germany, France, Australia had framed their national personal data protection legislation. In the 1980’s Canada, the UK, Australia and various other countries joined this ‘privacy club’. In 1995, the European Union adopted its influential privacy directive, for eventual ‘transposition’ in to the legal systems of all member countries. In the present chapter of the thesis the researcher is trying to discuss Comparative International development of Privacy Protection.

She tries to discover what forms of privacy protection are readily accepted in each country and what different government agencies did and did not define rules for themselves in protecting people’s interest in treatment of their privacy protection. What are those international agreements whose precepts have inspired National Privacy Codes around the World?

5.2 United States

American legal and philosophical thinking about privacy begins with Samuel Warren and Louis Brandeis’s 1890 Harvard Law Review article in which they argued that the Common law protected a ‘right to privacy’ and that ‘the right to life has come to mean the right to enjoy life’, ‘The right to be let alone’. They anchored the right to privacy in the common law protection for intellectual and artistic property-arguing that this protection was not based on
private property but instead on the concept of an inviolate personality. Privacy, or the ‘right of the individual to be let alone, was similarly protected as a part of the inviolate personality.’

The next major step in legal thinking on privacy is William Prosser’s article on privacy in which he concluded that a right to privacy, ‘in one form or another’, was recognized in four different tort protections: intrusion, disclosure, false light and appropriation. He viewed privacy as a common term for a number of different ways in which the ‘right to be let alone’ might be invaded.

The United States Constitution makes no explicit mention of the right to privacy. However, over time the Supreme Court has recognized a number of Privacy rights deriving them from the first, third, fourth, fifth, ninth, and fourteenth Amendments. These Constitutional Protections only apply to government action; they do not restrict private sector or individual actions or provide any protections against privacy invasions in those contexts. Under the first Amendment and due process clause of the fifth and fourteenth, the court has upheld a number of privacy interest including associational privacy, political privacy and the right to anonymity in public expression.

The most direct expression of the right to Privacy can be found in the US Constitution’s fourth Amendment, the fourth Amendment states:

“The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizure, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized.”

The purpose of the amendment was to protect people from arbitrary government intrusion into their liberty, privacy and possessory interests. The fourth Amendment encompasses two main ideas. First a government search and seizure must be “reasonable” Second, before embarking on a search or seizure, government actors should obtain warrant wherever possible, and warrant should be based on the principle of “Probable Cause”. Because the fourth Amendment apply only to “searches” and “seizure”, an investigative
method that falls with in neither category need not be reasonable and may be employed with out a warrant and without probable case, regardless of the circumstances surroundings its use.\textsuperscript{6}

The most important fourth Amendment case is Katz v. United States\textsuperscript{7}, A wiretapping case in which the court ruled that the fourth amendment protected people, not places, and did not require physical trespass or seizure of tangible material. In the concerning opinion, Justice John Marshall Harlan, developed a two part formulation to determine whether an individual had a ‘reasonable expectation of privacy’: First that a person have exhibited an actual (subjective) expectation of privacy and Second that the expectation is one that society is prepared to recognize as “reasonable”. Title 111 of the Omnibus Crime Control and Safe Streets Act 1968, and the Electronic Communications Privacy Act 1986, Congress has given more concrete meaning to the Fourth Amendment protection against unreasonable searches and seizures, requirements. The Fifth Amendment protection against self incrimination also provides a basis for a type of privacy protection. Judicial construction of Fifth Amendment protected privacy prohibits the government from compelling an individual to disclose incriminating personal information except on grants of immunity. Still, the contours of Fifth Amendment protected privacy may be broadly or narrowly drawn, depending upon the courts interpretation of the amendment’s underlying principles and policies.\textsuperscript{8}

As with Fourth Amendment, Boyd v. United States\textsuperscript{9} provides the watershed for a broad construction of personal privacy under the Fifth Amendment Boyd’s construction of the Fourth and Fifth Amendments foreclosed the possibility of overbearing governmental intrusions upon individual’s activities not only where the government searched and seized without warrant or elicited compelled disclosures of personal information, but also where the government through the use of administrative summons intruded upon individual’s privacy.\textsuperscript{10} With respect to personal information, the court has limited its protection to information that is in the possession of the individual,
not a third party and has waived protection for information that is part of a required record.

The broadest privacy right have been those adopted to protect reproductive privacy, which is conceptually different from information privacy, as it involves control over a personal domain in Griswold v. Connecticut\textsuperscript{11}, Eisenstadt v.Baird\textsuperscript{12}, and Roe v.Wade\textsuperscript{13} the court ultimately recognized a ‘right to privacy’ in the ‘Fourteenth Amendment’s concept of personal liberty and restrictions upon state action’. These protections however have not been extended beyond the sphere of reproductive privacy. For example in 1976, the court refused to expand the areas of personal privacy considered ‘Fundamental’ to include erroneous information in a flyer listing shoplifters. A year later, the court recognized for the first time two kinds of information privacy interest: ‘One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions. But in this instance, the court upheld a New York law that required the state to maintain computerized record of prescriptions for certain drugs because the state had taken precautions to protect computer security and had placed restrictions on disclosures from the records, thus minimizing the potential for personal information to be disclosed inappropriately.

The Supreme Court asserted in 1967, that the Fourth Amendment does not protect places, but rather it protects people and that the constitutional privacy right should not be dependent on the nature of the technology.\textsuperscript{14} Correspondingly in 1968, the U.S. congress established the Omnibus Crime Control and Safe Streets Act, which focused on telephone wiretaps. In 1986, it broadened to include digital electronic communications with the collection and dissemination of Information Act.\textsuperscript{15} Congress also tried to establish the principle that privacy rights should not depend upon the kind of technology that is used\textsuperscript{16} and thus enacted the Electronic Communications Privacy Act (ECPA), which made it illegal to intercept/disclose private communications,\textsuperscript{17} including key stroke monitoring, tapping a data line, rerouting electronic communication, and hacking”.\textsuperscript{18}
The Privacy Act of 1974, a major piece of legislation numbering over 9,000 words on the emerging concern of the new technological advances in the Computer Industry, serves as the most comprehensive, general federal statute on confidentiality.\textsuperscript{19} The law actually has roots from the House of Representatives sub committee on invasion of privacy in 1965.\textsuperscript{20} In response to Nixon Administration using political opponents' tax information made available through the Freedom of Information Act of 1966.\textsuperscript{21} According to the privacy Act, record keeping systems must not be kept secret and an individual must have the means to find out his record information and how it is used.\textsuperscript{22}

The Privacy Act, modified in 1980, eventually focused less on the government's accumulation of personal information and more on the flow of data in and out of computer. The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, later amended in 1986, made it felony to access classified information.\textsuperscript{23}

In 1988, the House created the Computer Matching and Privacy Protection Act 1988, which applies to the “Computerized Comparison of records for the purpose of establishing eligibility for a federal benefit programme or recouping payment or delinquent debts under such programmes”. Beside this, in 1988 Video Privacy Protection Act of 1988\textsuperscript{24} passed, which prohibits video stores from disclosing their customers name and addresses and the specific videotapes rented or brought by customers except in certain circumstances. Driver’s Privacy Protection Act of 1944\textsuperscript{25} restricts access to information maintained by State Departments of Motor Vehicles including name, address, telephone number, photograph, and medical or disability information.

Health Insurance Portability and Accountability Act of 1996\textsuperscript{26}, provides for standards protecting privacy of individually identifiable health information and establishes an offence of ‘wrongful disclosure’ with respect to Health Information Financial Modernization Act of 1999\textsuperscript{27}, commonly referred to as Gramm Leach Bliley (GLB) for its primary co-sponsors, requires financial institutions to send notice of their information practices to all customer. Inspite
of the low level of Protections conferred the effective data of the privacy provisions pushed back from November 2000 until July 2001. The year 2000 also saw the sole federal law governing information use online go in to effect. The Children’s Online Privacy Protection Act (COPPA), passed by Congress in 1998 and requiring Parental consent before information is collected from children under the age of 13, went into effect in April 2003. Protection for medical records was finally introduced in the US in 2001. In October 1999 Department of Health and Human Services issued draft regulations protecting medical privacy. The final rules were issued on December 20, 2000 and went into effect in April 2001. The large Number of exemptions provided limits the protection offered by the new rule. For example, patient information can be used for marketing and fund raising purposes. Doctors, Hospitals and Health services companies will be able to send targeted health information and product promotions to individual patients. There is also a variety of Sectoral Legislation on the State level that may give additional protections to citizens of individuals’ states.

5.3 United Kingdom

United Kingdom’s legal system has been gradual and evolutionary and describes its right in a negative fashion. The catch phrase “It is not what is good, its what is not said’ describes the traditional method of the British Constitution, which derives from several important document previously mentioned, Britain has taken the gradualist approach of it don’t broke don’t fix it: noticing that the government has always functioned efficiently by responding to current needs and so premeditated change is unnecessary.

Famous Englishman A.V. Dicey, author of the law of the Constitution believed it was futile to declare human freedoms without under pinning the rhetoric of liberty with effective means to protect them. Overall English law was more concerned with protecting property rights and physical right rather than social rights. Thus legislative emphasis was not on human liberties. In Britain precise legal remedies were made available through which citizens could secure freedoms, but without a general statement of rights. This idea
worked well until two changes occurred: Firstly, State incorporated more modern declarations of rights which were highly effective and usually required.

Judicial means to guarantee rights of all, Secondly the UK’s elective dictatorship allowed British government to be careless with legislative and administrative acts which infringed rights of citizen in favour of increasing power for the Central government.

A historical examination reveals that control of information emerged as a problem in Britain shortly before 1889, when the first Official Secrets Act was passed. As a Constitutional Monarchy, Britain repeatedly confronted the issue of having a central royal figure make confidential decisions with no public interference nor disclosures. In the face of increasing judicial power. The government had a vested interest in maintaining the traditional crown privilege, Official Secrets Act, and Ministerial accountability to ensure it continued control of information and power.

Historically, a British culture of secrecy upheld the Doctrine of Crown privilege, which states that courts have no authority to disclose the working of government crown privileges power were limited by the landmark case of Duncan v. Cammell Laird.

Another important case relating to privacy is widely known as “The Spycatcher Affair” in this case the British government pursued peter Wright, a former British secret service agent, for publishing his memories in Australia. The British government wanted to suppress the circulation of this information— but the disclosure did not provide a threat to Britain’s National Security, and consequently Britain lost the case. The trial revealed the illegal activities of Britain’s secret service and illustrated the government’s resistance in allowing public interest and freedom of the press to override Civil law of confidentiality.

Two additional examples demonstrate how Britain limited the freedom of expression and exchange of information. In 1983, Sarah Tisdall, a clerk for the Ministry of Defence, disclosed information concerning parliament’s evasion of discussing the arrival of American Missiles. Because she sent such documents to a newspaper, she faced a six month prison sentence. One year
later, a senior civil servant, Clive Pointing, informed parliament that ministers provided misleading information about a ship sinking during the Falklands war. Instead of rewarding him for his morals, he was prosecuted for leaking the information, although he was acquitted. In sum, a little over a decade ago, the Thatcher era was scarred with politically inspired attempt to circumvent press freedom: the Northern Ireland broadcasting ban; the injunctions against the publication of Spy Catcher by the retired intelligence officer, Peter Wright; the prosecutions of Clive Pointing and Sarah Tisdall for passing information which in other, more liberal systems would have been freely available; and a series of interventions against the makers and producers of television documentaries.\ldots if an informal system has broken down, it is certainly arguable that a formal system with precise and enforceable rules, is required to take its place.

In 1970, a committee on privacy was appointed under the chairmanship of Kenneth Younger. The Younger Committee which reported on privacy in the United Kingdom in 1972 observed that while privacy is widely recognized as a legally defensible right in the United States, it is not established as a concern principles of law and it has not significantly, contributed to respect for privacy in everyday life, especially by the mass publicity media. It is generally agreed that, to this point, the Common law of England and many other Common Wealth Common law jurisdiction knows no generalized right to privacy. In the parliamentary debate on the first of the private members bill on privacy introduced in the United Kingdom during the 1960's, Lord Mancroft’s Right of Privacy Bill, 1961. This Bill marked the beginning of a 23 year history which finally led to the successful passage of the Data Protection Act 1984. Lord Denning said that the law on privacy in the United States had evolved from the English Common law and that in England “The judges may well do it” The Younger Committee commented that Great Britain has less in its law aimed specifically at the invasion of Privacy than any other country whose law it had examined. Lord Dennings statement in the debate on the Mancroft’s Bill was very much in character, but it is very doubtful if the common
law of England would, at this time recognize or announce a general right of Privacy. As in England, so elsewhere in the common wealth, there has been no Common law development of a generalized right to privacy. Series of private member’s Bill, were introduced in the United Kingdom Parliament during the 1960’s, which dealt with privacy issues, Lord Mancroft’s Bill was concerned with privacy in the context of media other Bill have defined the right to privacy in very broad and general terms while others have listed specific diverse areas of conduct which are said to constitute breaches of privacy for example industrial espionage, electronic surveillance and data banks. In the United State there has been a great volume of writing and substantive legislative investigation and enactment of which Title III of the Omnibus Crime Control and Safe Streets Act 1968, dealing particularly with wire tapping and electronic surveillance is the most conspicuous recent example. More recently, a sincere effort is being made to enunciate positive rights in Britain, as opposed to freedom being defined as what’s left when the state has finished saying what you can not do. Opponents to the Diceyan view like Sir David Williams, an English champion of civil liberties, held the view that a legal system in which anything is permitted which is not forbidden is equivalent to the absence of principle masquerading as a principle.

In 1993, the government published a famous document, the white paper on “Open Government,” it explored excessive secrecy and suggested methods of how open government could be improved through the Code of Practice on Access to Government Information.

The code commits the government to providing information to the public regarding facts and fact analysis behind major policies and decisions. Details on policies, actions and decisions and explanation of government departments.

Of course they are the usual exemptions of official secrecy categories of defense and enforcement of the law, predictable categories of privacy, commercial confidentiality and individual confidentiality and the white paper
argued that right should be “brought home” to enforce convention rights in democratic court. 

The white paper however was not strong enough to preclude the desire of drafting the Freedom of Information (FOI) Bill, created by the New Labors party in 1997, and introduced to the House of Commons on November 18, 1999. A comprehensive piece of legislation was sought to create a coherent approach regarding Law of Information. The Freedom of information Act received Royal Assent on November, 30, 2000. A provision in the Act requiring authorities to produce publication schemes describing information they publish proactively, will be placed in earlier, starting with Central Government Departments in November 2002. Because the 2002 Act was characterized as weak legislation, the Scottish parliament created its own stronger bill. The Freedom of Information (Scotland) Act was passed by the Scottish Parliament on April 24, 2002 and enforced from December 31, 2005. The freedom of information Bill has advantages over the outdated white paper’s code: the statutory right of access to information, as opposed to a code has a major psychological as well as legal effect. The legislation will be fully retrospective, which will avoid problems with documents created fewer than thirty years ago. It also covers a wide range of organizations at all level of government.

Just before the freedom of information Bill came to the table, the Data Protection Act of 1998 was enacted because European Union (EU) law required implementation of a Data Protection Directive by October 24, 1998. The FOI Bill had to be drafted to fit into the legal landscape already shaped by the Data Protection Legislation.

Just before the Data protection Act, the UK confronted one of the most comprehensive Acts in its history: The European Convention of Human Right’s of 1998.

ECHR is one of the earliest and most important treaties passed by the Council of Europe, which is separate from the EU and has its own Court of Human Rights in Strasbourg; The Act makes three important changes: First it
makes it unlawful for a public authority like a government department local
authority or the police to breach the Convention rights unless an act of
Parliament meant it couldn’t have acted differently; secondly cases can be dealt
within a UK Court or Tribunal previously injured citizens had to go the
European Court of Human Rights in Strasbourg. Thirdly it says that all UK
legislation must be given a meaning that fits with the convention rights, if
possible. If a Court says that it is not possible, it will be up to parliament to
decide what to do.

British Parliament adopted into democratic law the ECHR on October 2,
2000. That day a speech was made by home secretary, Jack Straw MP, entitled
“Human Rights and Personal Responsibility New Citizenship for a New
Millennium”, which reflected on the post and predicted some fundamental
changes for the future.49

Straw recalled that the ECHR was created in response to world war two,
to ensure atrocities never took place again.

He reminded people that the world is now changing due to
Globalization, Information Technology (IT), The Internet Economic Progress,
Technical progress and movement of populations, but these new opportunities
also means new inequalities, undoubtedly social constrains may cause the new
legislation to be ineffective since challenging governmental actions in the court
is easier for rich people than poor people, the existence of constitutional
provision does not ensure it will be respected, and the constitutional clause are
short while the range of threats to freedom are infinite.50 To further support the
UK’s need for a Domestic Bill of Rights, in addition to procedural difficulties,
there are also substantive problems. The ECHR does not specify the right to
information from public bodies and is missing the right to privacy in relation to
due process.51 Article 8 of the Human Rights Act pertaining to Privacy, does
not give people a basic right to see information held by public authorities. The
FOI legislation will provide for the missing hole. Article 8 makes two main
assertions:
Firstly, everyone has the right for his private and family life, his home and his correspondence, and Secondly, there shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interest 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 as for the protection of the rights and freedom of others.\textsuperscript{52}

Article 10, of the ECHR guarantees the right to receive and impart education however there is no express guarantee for the right of access to information.

ECHR changes UK law in a number of ways. It creates a new mechanism for dealing with cases where convention and legislation conflicts a "Fast track" for dealing with legislation that violates ECHR.\textsuperscript{53}

5.4 Australia

While privacy issues are now featured prominently in daily news in Australia, the legal safeguards for personal information remain limited. Neither the Australian Federal Constitution nor The Constitutions of the six States contain any express provisions relating to privacy there is periodic debate about the value of a Bill of Rights, but no current proposals. The Constitution limits the legislative power of the Common Wealth (Federal) government, with areas not expressly authorized being reserved for the States. The Constitutionality of federal laws imposing privacy rules on the private sector has been questioned? But not so far challenged. Most commentators believe that the common wealth could found any private sector privacy law on a ‘cocktail’ of constitutional powers including those giving authority over telecommunications, corporations and foreign affairs (e.g. treaties).\textsuperscript{54}

Privacy law in Australia comprises a number of common wealth (federal) statutes. Covering particular sector and activities, some state or territory laws with limited effect and the residual common law protections. Which have very occasionally been used in support of privacy rights through action for breach of confidence, defamation, trespass or nuisance. The principal
Federal Statute is the Privacy Act of 1988.\textsuperscript{56} Which has four main areas of application and which gives partial effect to Australia's commitment to the OECD Guidelines and to the International Covenant on Civil and Political Rights (ICCPR). It creates a set of eleven information privacy principles (IPPs) based on those in the OECD Guidelines that apply to the activities of most federal government agencies. A separate set of rules about the handling of consumer credit information added to the law in 1989, applies to all private and public sector organizations.

The third area of coverage is the use of the government issued Tax File Number (TFN), where the entire community is subject to Guidelines issued by the privacy commission which take effect as subordinate legislation. The origins of the privacy Act where the protests in the mid-1980's against the Australia card scheme. A proposal for a universal national identity card and number. The controversial proposal was dropped but the use of the tax file number was enhanced to match income from different sources with the privacy Act providing some safeguards. Some controls over this matching activity were introduced in 1990.\textsuperscript{55} after several policy reversals, the selected conservative government introduced legislation to extend privacy protection to the private sector in April 2000. The privacy Amendment Act was passed in 2000. This law takes effect in December 2001. The law puts in place National Privacy Principles based on the National principles for fair Handling of personal information originally developed by the federal privacy commissioner in 1998 as a self regulatory substitute for legislation. The Act has been widely criticized as failing to meet international standards of privacy protection. Privacy expert Roger Clarke describes the Act as "The world's worst privacy legislation" or the Anti privacy Act.\textsuperscript{56} The NPPs impose a lower standard of protection in several areas than the EU directives. For example, organizations are required to obtain consent from customers for secondary use of their personal information for marketing purposes where it is "practicable", otherwise, they can initiate direct marketing contact. Providing they give the individual the choice to opt out of further communications. Controls on the transfer of personal information
overseas are also limited, requiring only that organization take reasonable steps to ensure personal information will be protected or "reasonably believes" that the information will be subject to similar protection as applied in the Australian law. In addition, the Act provides for a number of broad exemptions for employee records for example health information, contact details, salary or wages, performance and conduct, trade union membership, recreation and sick leaves banking affairs etc, media organizations and small businesses.57

There are also weaknesses in the enforcement regime including for example, allowing privacy complaints to be handled by an industry, appointed code authority with limited oversight by the commissioner. The Act does, however include an innovative principles of anonymity. Article 8 states that: Wherever it is lawful and practicable, individual must have the option of not identifying themselves when entering into transactions with an organization.

Genetic privacy was currently under joint review by the Australian Law Reform Commission and the Australian health ethic committee of the national health and medical research council, who had deliver their final recommendation by 30th June 2002. on June 20, 2001 the prime Minister Announced the establishment of a National digital data base of DNA and finger print samples in order to facilitate law enforcement.

The Telecommunicafion (Interception) Act of 197958 regulates the interception of telecommunications. A warrant is required under the Act and it also provides for detailed monitoring and reporting. However significant loopholes exist with in the legislation. There remains considerable uncertainly as to the position of email and other stored communications under the telecommunications laws. It is not clear which communications are subject to the Strict Interception Act safeguards and which only to lesser control of telecommunication Act.

Crimes Act, 198959 also contains a range of other privacy related measures such as offences relating to unauthorized access to computers, unauthorized interception of mail and telecommunications and the unauthorized disclosure of common wealth government information. In late
June 2001, the Government introduced draft legislation targeting online crime. The proposed Cyber Crime Bill 2001 would establish seven new computer offences (includes hacking, denial of service attacks, website vandalism spreading computer virus and the use of computer in offences such as stalking and fraud) with Jails terms up to 10 years. It would amend the crimes act to provide police with increased search and seizure powers including the authority to demand release of encryption keys or decrypted data. The Bill, which is likely intended to implement the substantive provision of the future council of Europe Treaty on Cyber Crime, has been widely criticized by civil liberties and computer users groups such as the Australian Computer Society and Electronic Frontiers Australia.

The Australian states and territories have varying privacy law. New South Wales, the most populous state, passed the Privacy and Personal Information Protection Act 1998, which applies privacy principles to most State government agencies although there are numerous and generous exemptions, and agencies can apply for codes of practice that can weaken the principles. The former privacy committee has been replaced by a part time privacy commissioner with a very small staff. The Act is based on a set of OECD style by a part time Privacy Commissioner. With a very small stuff. The Act is based on a set of OECD style information protection principles and requires all government and agencies to develop a privacy management plan demonstrating their compliance plans. It also allows government agencies to weaken the information protection principles, which form the foundation of the legislation. New South Wales has also recently enacted Work Place Video surveillance Act 1998. In August 2001; New South Wales become the first state to enact cyber crime legislation. The state of Victoria has enacted the Information privacy Act, 2000 which applies privacy principles to most state government agencies. There are relatively few exemptions and while there is provision for codes of practice, they can not weaken the principles. The Act created an office of privacy commissioner with a monitoring, enforcement and education role and to conciliate complaints. Victoria has, also passed the
Health Records Act 2001 to complement the information privacy legislation by requiring Victorian health service providers to handle health information responsibility. The Health Records Act also gives patients a right of access to their records held by private practitioners. The Victorian Law reform Commission received a reference in April 2001 to review the coverage of privacy law in Victoria, and is expected to focus at least on work place surveillance and surveillance in public places.

The government of the Australian Capital Territory, which used to be a local authority under common wealth (federal) law and was consequently covered by the Federal Privacy Act, achieved self government as a separated territory in 1989. However in 1997 the Australian Capital Territory government passed its own Health Records (Access and Privacy) Act,\(^{63}\) which applies to personal health information held by anyone, public or private sector. Its provisions are similar to those of the IPPs in the privacy Act, and supersede them for Act government agencies in this area of data handling. Queensland had a purely advisory privacy committee from 1984 to 1991\(^{64}\) and has a limited privacy statute. Covering the use of listening devices, credit reporting and physical intrusions into private property. In April 1998, after year long review parliamentary committee recommended privacy legislation at least for the public sector.\(^{65}\) the government has indicated that it intends to legislate but no time table has been set.

All of the states and the Australian Capital Territory also have freedom of information laws that include rights for individuals to access and correct personal information about them.

### 5.5 Canada

There is no explicit right to privacy in Canada's Constitution and charter of Rights and Freedoms\(^ {66}\) However, in interpreting Section 8 of the charter, which grants the right to be secure against unreasonable search or seizure, Canada's Courts have recognized an individual's right to a reasonable expectation of privacy.\(^ {67}\)
Some Canadian Judges have maintained that the preamble’s reference to “a constitution similar in principle to that of the United Kingdom” and more particularly a popularly elected house of commons preclude invasion of fundamental rights by provincial legislature and perhaps even by the Canadian parliament. But neither the privacy council nor an unambiguous majority of the Supreme Court has ever endorsed such liberation implications of the preamble.

In 1960, however, the Parliament of Canada enacted a statutory Bill of Rights, that recognize the existence “without discrimination by reason of race, national origin, colour, religion or sex,” of such rights a those to life, liberty and security of person and enjoyment of property, and the right not to be deprived there of without due process of law, “equality before the law, and freedom of speech, press, assembly, association and religion furthermore, the Bill directs judges to construe every federal statute, unless it explicitly states otherwise, not to abridge these rights.  

The Federal Privacy Act, of 1982 provides individuals with a right of access to personal information held by the federal public sector. In addition, the privacy act contains provisions regulating the confidentiality, collection, correction, disclosure, retention and use of personal information. Individuals may request records directly from the institution that has the custody of the information. The Act establishes a code of fair information practices that apply to government handing of personal records. However, its provisions can be ignored when another federal act allows for the processing of personal information. Individual can appeal to a federal court for review if access to their records is denied by an agency, but are not authorized to challenge the collection, use or disclosure of information.

Other federal legislations also have provisions related to privacy. The Telecommunication Act, 1993 has provisions to protect the privacy of individuals including the regulation of unsolicited communications. Also the Bank Act, Insurance Companies Act, and Trust and Loan Companies Act permit regulations to be made governing the use of information provided by customers. There are sectoral laws for video surveillance, immigration and
social security. The Young Offenders Act, regulates what information can be disclosed about offenders under the age of eighteenth while the corrections and conditional release Act, speaks to what information can be disclosed to victims and victims families. In addition, some form of legislation protecting consumer credit information. However the vast majority of information collected by the private sectors is on the provincial level and is not currently protected by provincial laws.

Canada has been a key player in the negotiations on cyber crime at the Council of Europe and G8 Lyon group level. A revised report issued by Mc Connell International LIC in January 2001 acknowledged Canada as “a leader in the international Height against cyber crime.”

There is great concern about the use of the Social Insurance Number (SIN) by the private sector and identity theft. A Parliamentary committee recommended in May 1999 that an Act Setting out limitations on the use of SIN be developed and that agencies use of the SIN should be documental. Human Resources Development Canada released it recommendation in November 1999 recommending that the SIN not become a national identifier because of severe privacy concerns and costs but it also recommending against new laws to prevent its use and expanding access to the social insurance register by users of the SIN to prevent fraud. In March 2000 Senator Sheila Finestone proposed a “Charter of privacy Rights” in March 2000. The character would create a broad constitutional right of privacy for all Canadians in all spheres and prevail over acts of parliament. According to senator Finestone: Under The Bill, every individual would be given the right to privacy. This right would include, but not be limited to personal privacy, which includes physical and psychological privacy; privacy of space, which includes freedom from surveillance; Privacy of communications, which includes freedom from monitoring and interception privacy of information, which includes freedom from collection, use and disclosure of their personal information by others. Any interference with an individual’s privacy would be an infringement of the individual’s right to privacy unless the interference is reasonably justified and
unless it is impossible or inappropriate to do so, the individual’s informed consent has been obtained.

A four part test is required to determine whether interference is reasonably justified the only permissible interference would be:

1. Where lawful;
2. Where necessary to achieve a compelling social interest that warrants limiting an individual’s privacy;
3. Where no other lesser measure will accomplish this objective, and
4. Where both the importance of objective and the beneficial effects of the interference outweigh the privacy loss.

The federal parliament approved Bill C-6 of the Personal Information Protection and Electronic Documents Act in April 2000. The Act adopts the CSA International Privacy Code. It does not apply to information collected for personal, journalistic, artistic, literacy, or non-commercial purposes. The law went into effect for companies that are under federal regulation, such as Banks, telecommunications, transportation, and businesses that trade data inter-provincially and internationally in January 2001, except with respect to medical records, which are exempted from the new law until 2002. In 2004, the Act covered all commercial activity in provincially regulated sectors unless the provinces enact; “Substantive similar” laws, such as Quebec’s law.

5.6 Ireland

Although there is not an express reference to a right to privacy in the Irish Constitution, the Supreme Court has ruled an individual may invoke the personal rights provision in Article 40.3 to establish an implied right to privacy. This article provides that “The state guarantees in its law to respect, and as far as practicable, by its laws to defined and vindicate the personal rights of the citizens.” It was first used to establish implied constitutional rights in the case of Mc Gee v. Attorney General which recognized the right to marital privacy. This case has been followed by others such as Norris v. Attorney General and Kennedy and Arnold v. Ireland. In the latter case the Supreme Court ruled
that the illegal wiretapping of two journalists was a violation of the constitution, stating:

The right to privacy is one of the fundamental personal rights of the citizen which flow from the Christian and democratic nature of the state. The nature of the right to privacy is such that it must ensure the dignity and freedom of the individual in a democratic society. This can not be insured if his private communications, whether written or telephonic, are deliberately and unjustifiably interfered with.\textsuperscript{86} Ireland has signed and ratified the European convention for the protection of Human Rights and Fundamental Freedoms.\textsuperscript{87} Unlike every other European signatory Country, Ireland has not incorporated this convention into National law. However, there have been announcements by the Government that the convention will soon be written into Irish law as a part of the Anglo-Irish peace talks. This would, for the first time, allow the provisions of the convention including the right to privacy, and the case law of the European Court of Human Rights to be relied on in Irish Courts. In 1988, the Data Protection Act, was passed in order to implement the 1981 council of Europe Convention for the protection of individual with regard to automatic processing of personal Data. The Act regulates the collection processing, keeping, use and disclosure of personal information processed by both the private and public sectors, but it only covers information that is automatically processed. Individuals have a right to access and correct inaccurate information. Information can only be used for specified and lawful purposes and can not be improperly used or disclosed. Additional protections can be ordered for sensitive data. Criminal penalties can be imposed for violations. There are broad exemptions for national security, tax, and criminal purposes. Misuse of data is also criminalized by the Criminal Damage Act 1991.\textsuperscript{88}

In 1977, the freedom of Information Act was approved and went into effect in April 1998. The Act creates a presumption that the public can access documents created by government agencies and requires that government agencies make internal information on their rules and activities available. The office of the information commissioner enforces the Act. According to The
Information Commissioners 1999 Annual Report, over 11,000 FOI requests in total were made to public bodies in 1999. The commissioner accepted 443 cases for review, of which 141 were completed. Ireland is a member of the Organization for Economic Cooperation and Development and has adopted the OECD Guidelines on the Protection of Privacy and Transborder flow of personal data. It is also a member of the council of Europe and as mentioned above it introduced the 1988 Data Protection Act to give effect to convention for the protection of individuals with regard to automatic processing of personal data.

Wiretapping and electronic surveillance is regulated under the Interception of Postal Packets and Telecommunications Messages (Regulation) Act. The Act followed a 1987 decision of the Supreme Court ruling that wiretap of journalists violated the Constitution. In April 1998, the Gardai investigated allegations that several journalists who had uncovered a scandal at the National Irish Bank had their cellular phone conversations intercepted. In its June 1998 Report on “Privacy, Surveillances and The Interception of Communications,” the law reform commission recommended legislation to make illegal the invasion of a person’s privacy through secret filming, taping and eavesdropping and the publication of information received from such surveillance. News stories this year carried reports of Ireland joining the controversial surveillance system known as ECHELON. In August 2001, the Irish Government expressed support for the controversial proposal by the EU Telecommunications council on Data Records Retention by communications operators.

Ireland is recognized as having the most modern copyright and electronic signature law in Europe. In July 2000, the E-commerce Act, was implemented granting legal recognition to e-signatures, e-writings and e-contracts. The copyright and related rights Act, which permits surprise searches and enact stiff penalties against software theft, came in to force in November. Ireland’s implementation of the EUSE commerce directive appears to make it the only European country to place the burden of opting out ‘spam’ on the
This legislation has enabled Ireland to promote itself as an attractive e-commerce, legislation.

5.7 Germany

While the German Constitution does not create a general right of privacy, three of its provisions do, however, protect privacy interests. The first is Article 2, of the German Constitution which guarantees the right to free development of personality. The second is Article 10, which protects the privacy of post and telecommunications. The third, finally, Article 15 the guarantee of the inviolability of the home under Article 13.

The year 1983, marked a watershed moment in the privacy Jurisprudence of the federal republic of Germany. It was the year in which the German federal Constitutional Court, in a remarkable display of Judicial activism, suspended the execution of a census under the Federal Census Act of 1983 pending a decision on the Act’s Constitutional validity, the Constitutional court formally acknowledged an individual’s right of information self determination that derived from the textual authority of Article 1(1) and 2(1) of the German Constitution, which make human dignity and personality inviolable. In a momentous decision, the Constitutional Court struck down the sections of the census law empowering the combination of statistical data and a personal registry, which could lead to the identification of persons and violate the core of the personality right. While most of the Act’s provisions were sustained, the court stressed the need to close all loopholes in the census law, which might lead to abuse in the collection, storage, use and transfer of personal data.

Germany has the distinction not only of having a well founded ‘right of informational self determination but also of being a pioneer in the field of data privacy legislation. Germany today has one of the strictest data protection laws in the European Union. Infact, the world’s first data protection law was passed in the German state of Hessel in 1970. In 1977, a Federal Data Protection Law followed, which was amended in 2002 to conform to the EU data protection directive. The General purpose of this law is to "Protect the individual against
violations of his personal rights by handling person-related data." The law covers collection processing and use of personal data collected by public federal and state authorities and by non-public offices, if they process and use data for commercial or professional aims. Germany was slow to update its law to make it consistent with the EU data protection directive, under the terms of the directive Germany should have harmonized its law by October 1998.

The European commission announced in January 2000, that it was going to take Germany to Court for failure to implement the directive. An amending bill was approved by the Government on June 14, 2000 and finally passed in to law in May 2001.\textsuperscript{99}

The 2001 revisions to the BDSG include regulations on transmitting personal data abroad, video surveillance, anonymization, Smart Cards and sensitive date collection. It grants data subject’s greater rights of objection. It also states that companies must now appoint a data protection officer if they collect, process, or use personal information, that databases collecting such information must be registered with Germany and that consent from the individual whose data is collected is required after full disclosure of data collection and its consequences.

Another important federal law in Germany is the G-10 law, which imposes limitation on the secrecy of certain communications. The G-10 law was amended in 2001 to require that service providers give law enforcement the means to monitor data as well as voice lines.\textsuperscript{100} Officials are trying to convince internet providers to self-regulate content, and European ISPs and data protection commissioners continue to resist demands from police agencies that they allow expanded surveillance of e-mail and store related data. Wiretapping is also regulated by the G-10 law and requires a court order for criminal cases.\textsuperscript{101}

After a fiercely fought six year political debate, a two-third majority of the German Parliament eventually approved a change to section 13 of the Constitution in April 1998, making it legal for police authorities to place bugging devices even in private homes. The change was the provision for the
enhancement of the fight against organized crime, "Which became effective in 1999. Germany is a member of the Council of Europe and has signed and ratified the Convention for the protection of individuals with Regard to automatic processing of personal data. It has signed and ratified the European convention for the protection of Human Rights and Fundamental Freedoms. It is a member of the organization for economic cooperation and development and has adopted the OECD Guidelines on the protection of privacy and Transborder flows of personal data.

5.8 Recapitulation

The concept of privacy differs from nation to nation in terms of the impact of culture on interpersonal relations. Indeed the law of a nation reflects and recognizes its fundamental norms. Right to privacy has been developing in many countries of the world to meet the needs to protect the individual from unreasonable intrusions in to areas of intimate concern. Globally, the right to privacy is one of the most carefully guarded rights, especially in an age where vast amounts of personal Information is provided, used, traded and even stolen.

An originating point of reference in the process of assessing an information privacy law would involve examining the US Federal privacy statute an ‘ideal privacy law’ that has kept pace with the rapidly evolving facets of individual privacy, since its inception in 1974, still the most comprehensive federal privacy legislation in the United States. Thus despite the fact that the US federal privacy statutes seem to be a fairly comprehensive statute with regard to securing, protecting and use of personal information relating to individuals due to contemporary technological developments and the emergence of newer and still evolving facets of individual privacy, the United states Government has enacted various legislations that are seemingly adequate in the efforts to conserve and protect individual privacy.

The United States Government has dealt in full measure with these emerging privacy issues by enacting a slew of statutes and legislations and making concerted efforts towards the conservation of individual privacy some of the key legislations enacted by the US Government are the Bank Secrecy

It may hardly be doubted that the lack of a clear legal remedy in respect of the non consensual disclosure of personal information are one of the most serious lacunae in United Kingdom is increasing day by day. United Kingdom does not have a written constitution or a specific law on privacy. However, in 1998, the parliament approved the Human Rights Act intended to incorporate the European Convention on Human Right, into domestic law, a process that will establish an enforceable right of privacy. The Act came into force on October 2, 2000.

There are also a number of other laws containing privacy components, most notably those governing medical records and consumer credit information. Other laws with privacy components included Rehabilitation of Offenders Act of 1974.


The privacy picture in the UK is mixed is at some levels there is strong public recognition and defense of privacy. There has been a proliferation of CCTV cameras in hundreds of Towns and cities in Britain.
In addition to these commitments the UK is a member of the Organization for Economic Cooperation and Development and has adopted the OECD Guidelines on the protection of privacy and Transborder flows of personal Data.

While privacy issues are not featured prominently in the daily news in Australia, the legal safeguards for personal information remain limited. Privacy law in Australia comprises a number of common wealth (federal) statutes covering particular sector and activities, some state or Territory laws with limited effect and the residual common law protections, which have very occasionally been used in support of privacy rights through actions for breach of confidence, defamation, trespass or nuisance. The principal federal statutes is the Privacy Act of 1988 which has four main areas of application, which gives partial effect to Australia’s commitment to the OECD guidelines to the International Covenant on Civil and Political Rights (ICCPR), Article 17, creates a set of eleven Information Privacy Principles (IPPs) based on those in the OECD guidelines that apply to the activities of most federal Government Agencies. In November 1999, the Australian Security Intelligence Organization Legislation Amendment Act 1999 was passed by the common wealth parliament.

There is no explicit right to privacy in Canada’s Constitution and Charter of Rights and Freedom. However in interpreting Section 8 of the charter, which grants the right to be secure against unreasonable search or seizure Canada’s Courts, have recognized an individual’s right to a reasonable expectation of privacy. The federal parliament of Canada approved the Bill C-6 The Personal Information Protection and Electronic Documents Act in April 2000. The Act adopts the CSA International Privacy Code.

Canada appears to have fashioned its private sector privacy law with an eye to achieving ‘adequacy’ by EU standards and there by forestalling trade disputes like the controversy that later nearly triggered a trade war between the USA and the EU over export of European personal data to America.
In Irish Constitution there is no express reference to a right to privacy, the Irish Supreme Court has ruled an individual may invoke the personal rights provision in Article 40.3.1 to establish an implied right to privacy this article provides that "The state guarantees in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of citizens."

Ireland has signed and ratified the European convention for the protection of Human Rights and Fundamental freedoms.

The freedom of Information Act was approved in 1997 and went into effect in April 1998. Ireland is a member of the Organization for Economic Cooperation and Development and has adopted the OECD guidelines on the protection of privacy and Transborder flows of personal Data. It is also a member of the Council of Europe and as mentioned above it introduced the 1988 Data Protection Act to give effect to Convention for the protection of individuals with regard to Automatic Processing of Personal Data.

Lastly as in other prosperous countries both state and private organization in Germany maintain a vast variety of data systems on private persons. The world’s first data protection law was passed in the German Land of Hessen in 1970. In 1977 a Federal Data Protection Law (BDSG) followed, which was reviewed in 1990, amended in 1994 and 1997. The general purpose of the law is to protect the individual against violations of his personal right by handling person-related data.

Even with the adoption of legal and other protections, violations of privacy remain a concern. In many countries, laws have not kept pace with the technology leaving significant gaps in protection. In other countries, law enforcement and intelligence agencies have been given significant exemptions. Finally, without adequate oversight and enforcement, the mere presence of a law may not provide adequate protection.

The current situation is that, despite the existence of the legislative framework and the efforts of National and International Data Protection Authorities and bodies, privacy abuse continues on a vast and persistent scale.
Notes & References

3. James S.B. Rule and Graham Green leaf, "Global Privacy protection" (The first Generation) Published by Edward elgar Publishing Ltd. at p. 52.
5. United States Constitution, Fourth Amendment.
6. Redefining the Right to be let alone: Privacy rights and the constitutionality of technical surveillance measures in Germany and the United States by Nicole E. Jacoby Alston & Bird, LLP (2006) at p.3
8. Supra Note 3.
9. 116 US. 616 (1886).
10. David M.O’ Brein, “Privacy law and public policy” published by Praeger publishers U.S.A., (1979) at p.113
11. 381 U.S. 479 (1965).
15. Guchtenerire and Mochmann, “data protection and data access” p 127.
16. Cavazos and Morin, Cyber space and the law, p.17.
17. Cavazos and Morin, “Cyber space and the law” at p.23.
18. Supra Note 10 at p.124.
20. Id 23.
22. Ibid.
23. Flaherty, protecting privacy in surveillance societies, p.358.
29. FTC Privacy pages <http://www.ftc.gov/privacy/index.html>
smith and privacy. Journal.,<http://www.epic.org/privacy/ consumer
/states.html>.
32. Short Civil Liberty p.364.
33. Supra Note 31 at p. 125-126.
35. TALLER, 587 (HL. 1939).
36. Debra L. Silverman, Freedom of information: Will Blair be Able to
Break the walls of secrecy in Britain? “Washington college of Law,
American University. The American University Law Review 1997 <
web. lexis. nexis. com / universe /document? Dateseg =1& -last
37. Jallyon Jenkins, “Official secrets in the UK A model for the EU?”
April 2003.


44. Supra Note 32 at p. 435.

45. Supra Note 43 at p. 300.

46. Ibid p. 257.

47. Ibid p. 303.


49. Ibid.


51. Black burn, Towards a constitutional Bill of Rights for the United Kingdom p 1028.


53. Supra Note. 43 at 256.


64. Privacy committee Act 1984.


67. Hunter V. Southam, 2 supreme court reports 2 (1984) 159-60

68. Mishra, Govind, „Right to privacy in India” Preeti Publication 1994 at pp. 132, 133.


71. Bank Act C-46, Sections 242, 244, 459.

72. Insurance Companies Act Sections 489, 607.

73. Trust and loan companies Act Section 444.

74. Criminal Code C-C-46, Section 487.


76. Old Age security Act, C.O-9, 5.33.01.
77. Young offenders Act, C. 4-1, S. 38.

78. Correction and Conditional Release Act, 1992, C 20, 5 -26, 142

79. Canadian Cyber Crime laws are among the strongest”, Mc Connell
Mc Connell international. com/press room/ 20010102

80. HRDC, A commitment to improvement: The Government of
Canada’s social insurance number, December 1999.

81. The Hon Sheila Finestone, P.C charting our future together:
consolation on a draft charter of privacy rights, March9, 2000
<http://www.itinc. net/fipa/finestone1.htm>.

82. Bill C-6 Personal information protection and Electronic Documents.
Act < http:// www. parl.IC.Ca/36/2/ parlbus/ chambus/ house bills/
government /C-6/C-6-4/C-6 _Cover - E.html>.

83. 1974 IR 284.

84. 1984 IR 36.

85. 1987 IR 587.


laws and development at p. 131.

irl gov. ieoic/oic/report 99/pub.html).

90. Signed 18/12/86. Enacted 25/05/90. Entered into force 01/08/90
<http:// conventions. coc.int/>.

91. “Gardai to Investigate surveillance Allegations,” The Irish Times
April 18, 2000.

92. The phoenix, May 5, 200, vol. 18 No. 9, p. 20.

93. “Cyber champion award presented to Taiseach , “The Irish Times
October 10, 2000.

94. Republic pul ‘spam’ Burden on the consumer “The Irish Times,
95. German Constitution, Article 2 states: "(1) every person shall have the right to free development of his personality in so far as he does not violate the rights of others or offend against the constitutional order or the moral law. (2) Every person shall have the right to life and to physical integrity. The liberty of the individual shall be inviolable. These rights may be inferred with only pursuant to a law."

96. German Constitution Article 13.

97. The Court noted that the right of information self determination might be limited for reasons of compelling public interest. Balancing the individual right against the legitimacy of a general census for social planning, the court directed the legislature to specify the purposes and conditions of data gathering and adopt organizational and procedural safeguards to protect privacy.


100. Germany: new law allows more extensive government monitoring of phone calls and e-mail, world socialist web site, February 20, 2001.

101. G-10 law of the Germany.