6 Cybercrime and Cybersecurity: The Legal Perspectives

Learning Objectives

After reading this chapter, you will able to:

- Understand the need for cyberlaws, especially in the Indian context.
- Understand how the laws of different jurisdictions across the world compare against a single benchmark.
- Get an overview of the European Union (EU) legal framework for information privacy to prevent cybercrime.
- Understand legal position on cybercrime with focus on the Indian scenario.
- Learn the strengths and weaknesses of the Indian IT Act along with the amendment to the Act.
- Understand Indian IT Act in cybercrime perspective.
- Understand the meaning of digital signature, public-key infrastructure as well as the implications of digital signature in the context of the Indian IT Act.
- Learn about electronic records and their admissibility in the courts.
- Get an overview of challenges faced in punishing the cybercriminals.
- Understand the Indian challenges in the fight with cybercrime seen from the legal angle.

6.1 Introduction

It is said that cybercrime is the *largest illegal industry*. Cybercrime involves massive, coordinated attacks against the information infrastructure of a country. In this chapter, we want to bring forth the point that knowledge of cyberlaws is essential for people who may directly or indirectly interact with networked services either over the Internet or other proprietary networks of businesses and enterprises of any other types – banks, stock brokers, intra-company and inter-company information exchange systems, etc. We have explained the term *cyberlaw* later in this chapter. It is also essential for those who are involved in heavy and indiscretionary use of social networking sites[1] (e.g., Orkut, Facebook, Big Adda, etc.). We want to understand the meaning of the term *digital evidence* given that the Indian Information Technology Act (ITA) 2000[2] and its modification (ITA 2008) mention about *evidence*. In the original ITA 2000,[3] there is a mention about "special provisions as to 'evidence relating to electronic record' and 'admissibility' of electronic records." We also explain the legal position on cybercrime based on Section 1.7 of Chapter 1 and discuss the topic of legal aspects of cybercrime into further details. Although the Indian legislations are important for people in India, we must not lose sight of the world scenario – it is important for global businesses. Therefore, while maintaining focus

on the Indian ITA 2000 and subsequent amendments in year 2008, that is, ITA 2008, this chapter also provides an overview of cybercrime legislations in other countries/regions.*

From an Indian perspective, we have provided adequate focus on the Indian ITA 2000 (previously known as the IT Bill) and its recent amendments known as the ITA 2008 (Amendments to the IT Act that came toward the end of year 2008).

Chapter 1 is the background to appreciate the concepts presented in this chapter. An overview on cybercrime is provided in Chapter 1; many fundamental terms with regard to cybercrime are explained (see Box 1.1) in that chapter along with the classification of cybercrime: (a) an Indian perspective on cybercrime is provided in Section 1.7; (b) reference to the Indian IT Act in the context of cybercrime is provided in Section 1.8; (c) a discussion on the global perspective on cybercrime, with implications for organizations and individuals, is available in Section 1.9. With this background, Fig. 6.1 presents the paradigm for cybersecurity.

The concept of *trust seals* mentioned in Fig. 6.1 is a very important one for electronic commerce (E-Commerce) era. (This concept is explained in Ref. #1, Books, Further Reading.) Figure 6.1 shows the *identify theft* group of crimes (identity theft is discussed in Chapter 5). Countries that are members of the EU[4] (European Union) have very stringent laws for protection of individual privacy and data privacy. (Readers interested in greater details of data privacy should refer to Ref. #2, Books, Further Reading.) The bottom block in Fig. 6.1 points to the IT infrastructure in organizations (government organizations as well as private or other kinds of organizations). From attack perspective, the intrusion detection system (IDS) are important. Readers new to IDS can refer to Ref. #3, Books, Further Reading.

For the benefit of those who are reading this chapter without having referred to Chapter 1, cybercrime definitions are mentioned here as well. Cybercrime spans not only state but national boundaries as well. Perhaps we should look to international organizations to provide a standard definition of the crime. At the

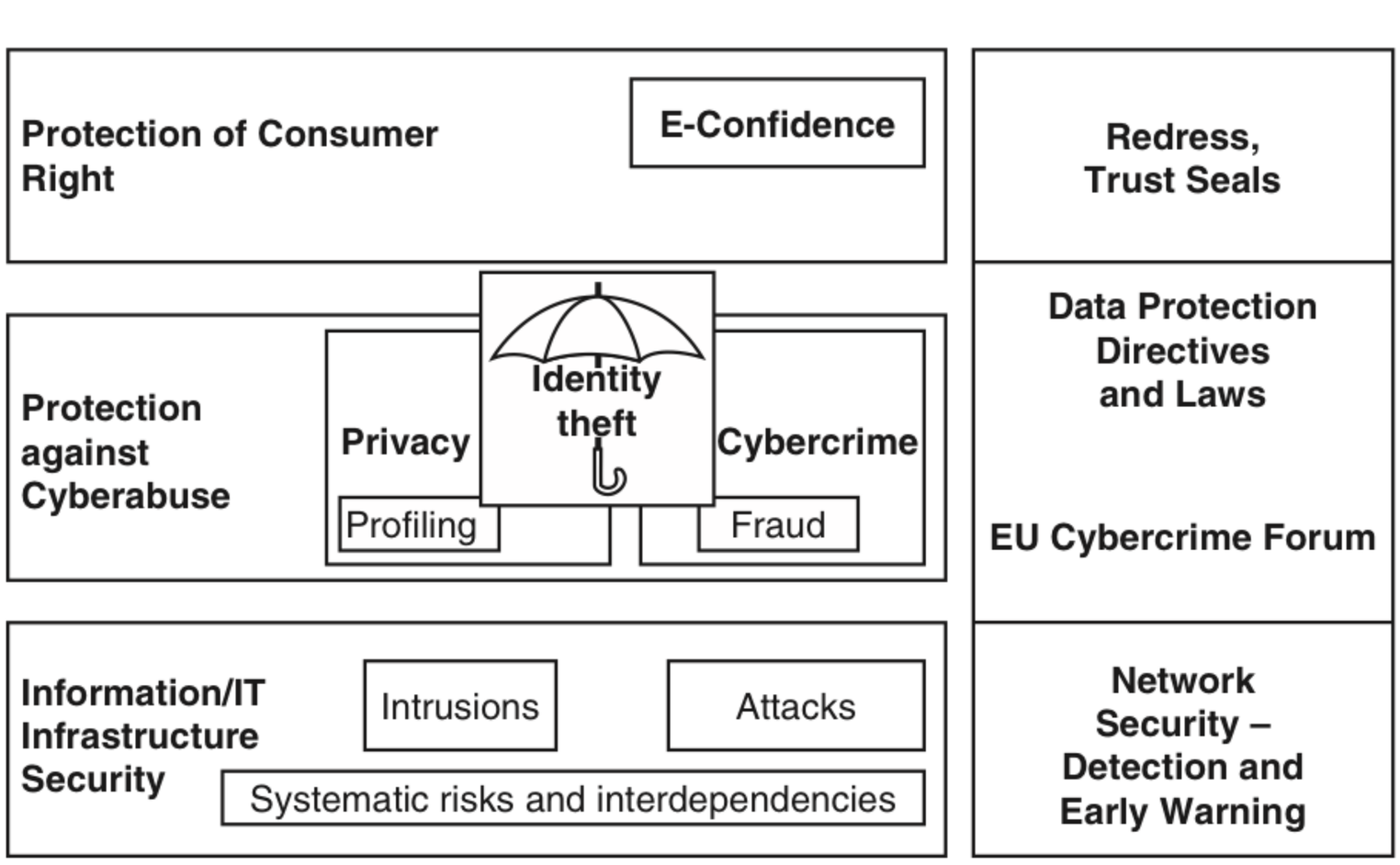

Figure 6.1 | A cybersecurity perspective: European Union.

*caveat – although this chapter provides discussion on the legal aspects of cybercrime, it is important for readers to appreciate that the contents of this chapter are NOT a substitute for consulting the legal experts/legal professionals when a particular case of cybercrime arises with which readers may be confronted or involved with. This is because the legal aspects presented here are based on our awareness and research and by no means, it is claimed to be the perfect or complete knowledge of legal parameters for defending a case. Readers should refer to the paper copy of ITA 2000 and ITA 2008 for exact wordings.

Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cybercrime was broken into two categories and defined as:

1. **Cybercrime in a restrictive sense (computer crime):** It is referred to any illegal behavior that is carried out by means of electronic methods targeting the security of computer systems and the data processed by them. This can be considered as a narrow definition of the term *cybercrime*.
2. **Cybercrime in a general sense (computer-related crime):** It is referred to any illegal behavior that is committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, and offering or distributing information by means of a computer system or network. This can be considered as a broader definition of the term *cybercrime*.

These definitions are complicated by the fact that an act may be illegal in one nation but not in another. There are more concrete examples, including

1. Unauthorized access to computer (see Box 6.1);
2. causing damage to computer data or programs;
3. an act of computer sabotage;
4. doing unauthorized interception of communications;
5. carrying out computer espionage.

Box 6.1 Degrees of Unlawful Access to Computer

In Chapter 1 we mentioned about classification of cybercrimes; one of the cybercrime types mentioned there is *unauthorized accessing of computer* under the broad category of cybercrime called *cybercrime against property*. Unauthorized access to a computer is most commonly known as *hacking*. Generally, hacking takes place when a person either illegally gains access to a computer system by taking advantage of or overcoming existing security (i.e., passwords and firewalls); or a person exceeds authorized access of a computer. Similarly, *cracking* is when a person gains unauthorized access (or "hacks") into a computer in order to commit a crime within that computer system. From the legal perspective, computer hacking and cracking statutes are titled *Unlawful Access to a Computer*. Such acts are only crimes when done without the consent of the owner. For framing different legal charges, the breakdown of varying degrees of unlawful access to a computer is as follows:

First-degree access: The crime of unlawful access to a computer is of first degree when a person accesses, causes to be accessed or attempts to access a computer, computer system and computer software for the purpose of defrauding or obtaining money, property or services by fraudulent pretense. Such a person is guilty of unlawful access in the first degree. This crime is a *Class C felony*.

Second-degree access: Unlawful access is of second degree when a person accesses, causes to be accessed or attempts to access a computer, computer system and computer software, and the crime results in damages or losses of value considered high enough by the law (the value would vary from country to country). This crime is a *Class D felony*.

Third-degree access: Unlawful access is of third degree when a person accesses, causes to be accessed or attempts to access a computer, computer system and computer software, and the crime results in loss or damage of less than the value that is considered "high" by the prevailing law in the country (this amount varies from country to country). This is a *Class A misdemeanor*.

Fourth-degree access: Unlawful access is of fourth degree when a person accesses, causes to be accessed or attempts to access a computer, computer system and computer software, but there is no loss or damage. This is a *Class B misdemeanor*.

First-degree access is the most serious one from the legal perspective. Relate this to item serial number 5 of Table 1.1 in Chapter 1.

Box 6.1 Degrees of Unlawful . . . (*Continued*)

Computer trespassing is another term to consider. A person is guilty of computer trespass in the second degree if the person, without authorization, intentionally gains access to a computer system or electronic database of another under circumstances not constituting the offense in the first degree.

In other words, *computer trespassing* involves using a computer with knowledge that such use is without authority and with the intention of: (a) deleting or in any way removing, either temporarily or permanently, any computer data; (b) obstructing, interrupting or in any way interfering with the use of a computer program or data and (c) altering, damaging or in any way causing the malfunction of a computer.

In reference to the above-mentioned term *unauthorized access*, note that the law considers *computer trespass* to be a crime. For example, according to Sections 18.2–152.4 of *Virginia State Criminal Law*, computer trespass is deemed to have occurred when any person uses a computer or computer network without authority and with the intent to:

1. Temporarily or permanently remove computer data, computer programs or computer software from a computer or computer network;
2. cause a computer to malfunction regardless of how long the malfunction persists;
3. alter or erase any computer data, computer programs or computer software;
4. effect the creation or alteration of a financial instrument or of an electronic transfer of funds;
5. cause physical injury to the property of another; or make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs or computer software residing in, communicated by or produced by a computer or computer network shall be guilty of the crime of computer trespass which shall be punishable as a Class 1 misdemeanor.

In the US, as per *Virginia State Criminal Law*, if such an act is done maliciously and the value of the property damaged is $2,500 or more, the offense shall be punishable as a Class 6 felony. (The term *felony* means an offense or a crime or a criminal act or law breaking/wrong doing.)

All forms of cybercrime are increasing rapidly – cybercrime is the latest and perhaps the most complicated problem in the cyberworld; in a way, it is a bane of Information and Computer Technology (ICT). It is said that the US still produces more malware, Spam and viruses than any other country in the world. Illicit IT jobs are increasingly scattered across an anarchic and international Internet, where labor is cheap, legitimate IT jobs are scarce and scammers are insulated from the laws. Maintaining legal, political and technological standards on the Internet is increasingly important, as cyberattacks take a greater toll. In year 2007, Computer Security Institute in the US conducted a survey[5] according to which, the average financial loss suffered by individual US corporations, agencies and institutions due to cyberattacks was US$ 350,424. This loss in figure turns out to be more than double compared to that in the year 2006. Total losses from cyberattacks were $66.9 million, with financial fraud incurring the most damage at $21.1 million in total losses. Chapter 1 provided the Indian statistics on cybercrime (refer to Tables 1.1–1.4). This is the background for understanding the legal landscape on cybercrime.

6.2 Cybercrime and the Legal Landscape around the World

Before getting into India-specific discussion, we discuss here the world scenario considering the following countries: the US, Europe, Canada, Asia-Pacific and Africa. First, let us examine the term *crime* under the legal microscope. *Crime* is a legal concept and has the sanction of the law. Crime or an offense is "*a legal*

wrong that can be followed by criminal proceedings which may result into punishment." The hallmark of criminality is that it is breach of the criminal law. Box 6.1 describes various scenarios for the unlawful access to a computer system. We start with a broad view of the legislative analysis in the Asia-Pacific region, followed by a detailed examination of the legal status (with regard to cybercrime and privacy protection) in Australia, China, Hong Kong, India, Indonesia, Japan, Malaysia, New Zealand, Philippines, Singapore, Thailand, South Korea and Vietnam. From this discussion we will realize that the extent and nature of Internet safety, security and privacy legislation in the Asia-Pacific region varies widely. We will also have a discussion on federal laws in the US about cybercrime. Next, we will discuss the EU legal framework to prevent cybercrime.

One of the preconditions for development of the Information Society is for users to have confidence or "trust" in the reliability, security and integrity of electronic communications systems and computerized information processing systems. This is supported by much literature; for example, the work by researchers at the Carnegie Mellon University in their research paper *The Effect of Online Privacy Information on Purchasing Behaviour: An Experimental Study* (accessible at the link http://weis2007.econinfosec.org/papers/57.pdf) Individuals will be reluctant to use networks or systems they do not trust. If there is no trust, individuals will tend to either not disclose personal information or provide false information. Therefore, one critical component of the trust framework is *privacy protection* – the provision of assurances by means of law, technology design and industry practice that personal information will be collected, exchanged and used fairly. As far as the law is concerned, the Web, that is the World Wide Web (WWW), still resembles the *wild west*. Bringing about legal governance for behavior on the Web is a specialty evolving rapidly due to innovations on the Internet. Catching cybercriminals under the legal edifice is a challenge. This is so partly because there is "no central authority" that enforces cyberlaw when crimes are committed. Plaintiffs still turn to traditional law enforcement to solve problems.

6.2.1 A Broad View on Cybercrime Law Scenario in the Asia-Pacific Region

When we consider challenges involved in the Asia-Pacific region, for handling cybercrime, we realize that the challenges exist mainly due to the general lack of awareness of information security issues, the rapidly evolving complexity, capacity and reach of ICT, the anonymity afforded by these technologies and the transnational nature of communication networks. Consequently, only a few countries of the Asia-Pacific region have appropriate legal and regulatory frameworks to meet these challenges. Even where awareness is growing and where legislation may be adequate, capacity to use information security technologies and related procedures as well as to protect against, detect and respond effectively to cybercrime, and to assist other countries, is low. As a result, published cybercrime reports may represent only a small fraction of their incidence and there is a need for more accurate estimates of the prevalence of cybercrime.

Information privacy or data protection in this context is not about keeping personal information secret; rather, it is about creating a trusted framework for collection, exchange and use of personal data in commercial and governmental contexts. The *Fair Information Practices* (FIPs) are explained in detail in Ref. #4, Books, Further Reading. Data protection laws[6] permit, and even facilitate, the commercial and governmental use of personal data while providing to individuals (a) control over what to disclose, (b) awareness of how their personal data will be used, (c) rights to insist that data are accurate and up to date, and (d) protection when personal information is used to make decisions about a person.

Now let us consider the Australian Cybercrime Act 2001. The Australian Cybercrime Act 2001 came into effect in Australia in April 2002. This was the third time that a Federal Government has passed cybercrime legislation; previous legislation was passed in 1989 and in 1995. Each attempt was meant to reduce the gap between legislation and malicious online activity. However, Cybercrime Act 2001 is the subject of much

controversy as critics argue that it is too broad in jurisdiction, extends police powers too far and threatens to facilitate the unjust conviction of many Information Technology (IT) professionals. This Act provides too broad a definition of *cybercrime*. Much of the criticism is based on that excessively broad definition and the extent to which the Act has been left for interpretation by the courts. Let us take a glimpse of the Australian Cybercrime Act 2001. This Act introduces the following new offenses to the Criminal Code Act 1995.

1. The serious offenses under Division 477 are as follows:
   - *Section 477.1:* Unauthorized access, modification or impairment with intent to commit a serious offense.
   - *Section 477.2:* Unauthorized modification of data to cause impairment.
   - *Section 477.3:* Unauthorized impairment of electronic communication.
2. The other offenses under Division 478 are as follows:
   - *Section 478.1:* Unauthorized access to, or modification of, restricted data.
   - *Section 478.2:* Unauthorized impairment of data in a computer disk, etc.
   - *Section 478.3:* Possession or control of data with intent to commit a computer offense.
   - *Section 478.4:* Producing, supplying or obtaining data with intent to commit a computer offense.

Not surprisingly, the Australian Cybercrime Act 2001 has drawn considerable criticism: it criminalizes far too much and far too easily, leading to severe consequences for IT professionals. This problem arises primarily from the overly broad definitions adopted by this legislation, specifically the breadth of the terms defined (in the Cybercrime Act) has created an even broader scope of potential criminality. Among the most concerning aspects of the Act are the definitions of *restricted data* and *authorization*; the mental elements of the offenses and the actions that constitute an offense: unauthorized access, modification and impairment.

1. **Restricted data:** In order for data to be defined as *restricted*, it simply needs to be held in a computer that uses an access control system. However, it is NOT a requirement that the data itself is protected by an access control system; only the computer needs to be protected by the access control system. According to this definition, the requirement of *restricted data* can be too easily met, as almost all computers are protected by at least a password. Therefore, to be in breach of Section 478.1 of the Australian Cybercrime Act 2001, an individual simply needs to view almost any data without authorization, notwithstanding whether or not that data was secured. This is further complicated by the lack of explanation of what constitutes having "authorization."
2. **Authorization:** A key requirement for conviction, under any of the Division 477 offenses and half of the Division 478 offenses, is that access, modification or impairment is undertaken without "authorization." Yet the Australian Cybercrime Act merely states that the action undertaken must be unauthorized, without actually specifying what constitutes authorization. The Act does not, in any way, address situations where authorization may be disputed, revoked or granted conditionally. For example, if an IT professional is hired to undertake some work, and suppose that in the course of that work, the authorization granted to that person is disputed or revoked, then there may exist a basis for prosecution under Section 478.2 (of the Australian Cybercrime Act 2001) for "unauthorized access or modification to restricted data." The additional requirement of *restricted data* can be easily met, as explained above.

Now let us understand the powers granted by the Australian Cybercrime Act. Under the Act, new powers granted for law enforcement include:

1. The power to remove "a thing" to another place for the purpose of examination or processing to determine whether it may be seized under a warrant, if it is more practical, or there are reasonable grounds that the "thing" includes or is an evidence.

2. The power to "operate electronic equipment" at the warrant premises in order to access data (including data not held at the premises) if the police believe that the data (may) contains evidentiary material.
3. The power to require a person "to provide any information or assistance" that is considered reasonable and is necessary in order to allow the officer to make a copy of data from equipment that might contain evidential material.
4. The power to require a "person with knowledge of a computer or a computer system to assist access," etc.

In conclusion, we note that the enactment of the Australian legislation means that it is now possible that other well-intentioned actions by Australian IT professionals may be regarded as criminal activities. IT professionals must now take more care in the performance of their duties, and must be much more aware of how their actions may be construed, to avoid risk of prosecution for their well-intentioned actions. The Australian Cybercrime Act 2001 heralds an era of de facto censorship in research and development of computer science fields.

6.2.2 Online Safety and Cybercrime Laws: Detailed Perspective on the Current Asia-Pacific Scenario

The extent and nature of Internet safety, security and privacy legislation in the Asia-Pacific region varies widely. In this section, we are going to consider the legislative position in Asia-Pacific countries with regard to data privacy (impacted by most forms of cybercrimes such as, e.g., identity theft), Spam (unwanted mails) and online child safety (because this closely relates to COPPA). Our objective in this section is to gain an understanding of how the laws of different jurisdictions compare against a single benchmark. In some areas such as computer security laws and online child safety laws [such as the Children's Online Privacy Protection Act (COPPA),[7] also mentioned in Chapter 1)], there exist international norms on the best approach to regulation. For example, the Council of Europe's (CoE's) Convention on Cybercrime is widely regarded as the international norm on the criminalization of computer-related conduct, and the International Centre for Missing and Exploited Children (ICMEC) has developed authoritative model legislation that criminalizes the production of, and certain dealings with, child pornography.[8] This model has been adopted as the benchmark legislation for the computer security and online child safety matters. However, in other areas, such as privacy laws and Spam, there seem to be no international norms.

In the privacy arena, there are numerous regional norms, such as the *A*sia-*P*acific *E*conomic *C*o-operation (APEC) Privacy Framework and the EU's Data Protection Directive, but an international consensus on the best approach to data protection regulation has not yet been reached. However, CoE's Convention on Cybercrime[9] serves as the benchmark legislation (see Box 6.2). Titles 1, 2 and 5 of the CoE's Convention on Cybercrime serve as the benchmark legislation. The alignment status of various Asia-Pacific countries mentioned in Table 6.1 is in that benchmark reference.

Box 6.2 The APEC Framework on Privacy

Today belongs to "global economy" and information flows are vital to conducting business in a global economy. The APEC Privacy Framework promotes a flexible approach to information privacy protection for APEC Member Economies, while avoiding the creation of unnecessary barriers to information flows. The APEC Privacy Framework is a practical policy approach to enable accountability in the flow of data while preventing impediments to trade. It provides technical assistance to those APEC economies that have not addressed privacy from a regulatory or policy perspecitve.

Box 6.2 The APEC . . . (*Continued*)

The framework will enable regional data transfers to the benefit of consumers, businesses and governments. The framework provides clear guidance and direction to businesses in APEC Member Economies on common privacy issues and outlines the impact of these issues on the various legitimate business models. It does this by outlining reasonable expectations of the modern consumer on how their privacy interests should be protected.

There are nine principles to the APEC Privacy Framework:

1. Preventing harm;
2. integrity of personal information;
3. notice;
4. security safeguards;
5. collection limitations;
6. access and correction;
7. uses of personal information;
8. accountability;
9. choice.

Data is the digital currency that fuels the growth in many of today's economies. This framework will facilitate responsible information flows, which creates an essential basis for increased trade and E-Commerce to flourish. It enables government, business and societal benefits by developing domestic markets, improving efficiencies and economic growth, and attracting foreign investment, which also leads to developing local industry. The framework focuses on both domestic and international implementation of privacy standards for APEC Member Economies. It explores new ways of information sharing and cooperation across agencies and authorities to enable transfers of personal information across borders. The framework also provides specific examples of privacy situations and focuses its attention on practical and consistent information privacy protection within this context. The framework balances privacy with all relevant interests while according due recognition to issues of cultural and economic diversity that exist within the APEC Region.

Note: Privacy details are discussed in detail in Ref. #4, Books, Further Reading.

Computer Security Laws

The Australian, New Zealand, Singaporean, Taiwanese and Thai Governments have each enacted robust computer security laws that cover most of the core and computer-related offenses found in the CoE's Convention on Cybercrime. The computer security laws in China, Hong Kong, Japan and South Korea are moderately aligned with the Convention. The enacted laws in Malaysia, the Philippines and Vietnam are moderately to weakly aligned, respectively, with the Convention (see Table 6.1). Malaysia and the Philippines have enacted some computer security offenses; however, the focus of these offenses appears to be on unauthorized access and these countries still rely on their general law to criminalize a number of the acts prohibited by the Convention. Vietnam's implementation of the Convention's core, and computer-related fraud and forgery, offenses appears to be piecemeal and arises from the enactment of multiple, overlapping prohibitions in various instruments, including the Law on Information Technology 2006 and the Law on E-Transactions 2005.

In India, although the ITA 2000 prohibits many of the activities that constitute core offenses under the Convention, the IT Act does not, for the most part, criminalize these activities – it merely provides for significant liability in damages. This civil liability approach is unique in the region. India's Information Technology (Amendment) Bill 2006 (IT Amendment Bill No. 96 of 2000) was proposed to amend the IT Act to criminalize many of the Acts that constitute core offenses under the Convention but only where they are done "dishonestly or fraudulently." In September 2007, the Standing Committee on IT submitted its

Table 6.1 | Asia-Pacific region: Alignment of the countries enacted legislation with regard to the benchmark legislation

Favorable Alignment	*Moderate Alignment*	*Weak Alignment*
Australia	China	India
New Zealand	Hong Kong	Indonesia*
Singapore	Japan	—
Taiwan	Malaysia	—
Thailand	Philippines	—
—	South Korea	—
—	Vietnam	—

*No computer security laws have been enacted.

report on the IT Amendment Bill to address a number of substantive recommendations in respect of the bill. This resulted in the ITA 2008 (amendments to the Indian ITA 2000).

Indonesia's Bill on Electronic Information and Transaction (EIT) is weakly aligned with the Convention (refer to Table 6.1). Partly, this is due to its emphasis on unauthorized access and the protection of government and financial computer systems. Japan and China have also been considering updated cybercrime laws for some time now. The Japanese parliament, since 2004, has a long pending matter of amendment to the criminal code to criminalize the preparation, production, dissemination and use of computer viruses and malware; this has been pending along with a separate piece of legislation that seeks to implement Japan's remaining obligations as a signatory to the Convention on Cybercrime. China has drafted its "National Information Security Regulations." However, neither the content of these regulations nor the timeframe for their enactment is known. Table 6.1 shows the alignment position of the mentioned countries with regard to the CoE's Convention on Cybercrime as the benchmark.

This degree of alignment varies due to the range of Convention offenses covered by the enacted legislation and the restrictive way in which some of the Convention offenses are implemented (e.g., requiring that unauthorized access be obtained by use of a telecommunications line). Take the example of Hong Kong – its general criminal law seems to apply in several cases to computer-facilitated act that is criminalized by the Convention on Cybercrime. It is interesting to know that Hong Kong has enacted fewer offenses with regard to computer security, which is one of the aims to which the Convention is directed. Owing to lack of comprehensive computer security laws, jurisdictions such as Indonesia rely on the application of their existing laws to regulate conducts that are declared criminal by the Convention. Legislatures in Indonesia, India and the Philippines are currently considering comprehensive computer security laws. In India, as we know the IT Act has been amended. The Philippines' proposed Cybercrime Prevention Act of 2005 (HB 3777) is considered to be the most closely aligned with the Convention on Cybercrime. It almost identically reproduces the Convention's core offenses, computer-related fraud and forgery offenses, and ancillary liability provisions.

Data Privacy and Data Protection

Position on privacy laws also greatly varies in the Asia-Pacific region. Table 6.2 shows the alignment position with regard to the benchmark legislation that was mentioned earlier in this discussion. The Microsoft-drafted Model Privacy Bill serves as the benchmark legislation in data privacy arena (referred to as the *Model Bill*). Privacy mature organizations are regulated by prevailing privacy regulations in their respective countries. As such, and as per the FIPS, these organizations must provide a "privacy notice" before collecting "personally identifiable information" (PII). *Privacy notice* is a statement made to a data subject that describes how the

Table 6.2 | Asia-Pacific region: Alignment of the countries enacted legislation with regard to Microsoft Model Privacy Bill

Favorable Alignment	*Moderate Alignment*	*Weak Alignment*
—	Australia	India*
—	Hong Kong	Indonesia*
—	Japan	Malaysia
—	New Zealand	Philippines
—	—	Singapore*
—	—	South Korea
—	—	Taiwan
—	—	Thailand
—	—	Vietnam

*No data protection laws have been enacted.

organization collects, uses, retains and discloses personal information. Sometimes, a privacy notice is referred to as a privacy statement, a fair processing statement and even a privacy policy. Providing privacy notice is important to be entitled to use or disclose it for a secondary purpose. The privacy-regulated organization must obtain a prior consent of the data subject – either explicit, Opt-Out or implied – depending on several factors related to the privacy risk involved (see Fig. 6.2).

From privacy perspective, there are two kinds of information about individuals: *aggreated information* and *PII*. Aggregate information or statistical information is complied, that is not personally identifiable. Examples of aggregate information include, but are not limited to, demographics, domain names and website traffic counts. PII is any information that can be traced to a particular individual. Note that *aggregate information* is not considered as PII. For example, information indicating the number of visitors to a particular Internet site. Commonly known examples of PII are the "social security number" (SSN) in USA, personal account number (PAN) in India, name, E-Mail address, phone number, etc. Personal user preferences tracked by a website via a cookie are also considered personally identifiable when linked to other PII provided by a user online. The definition of PII may vary from organziation to organization. Some people in the IT industry

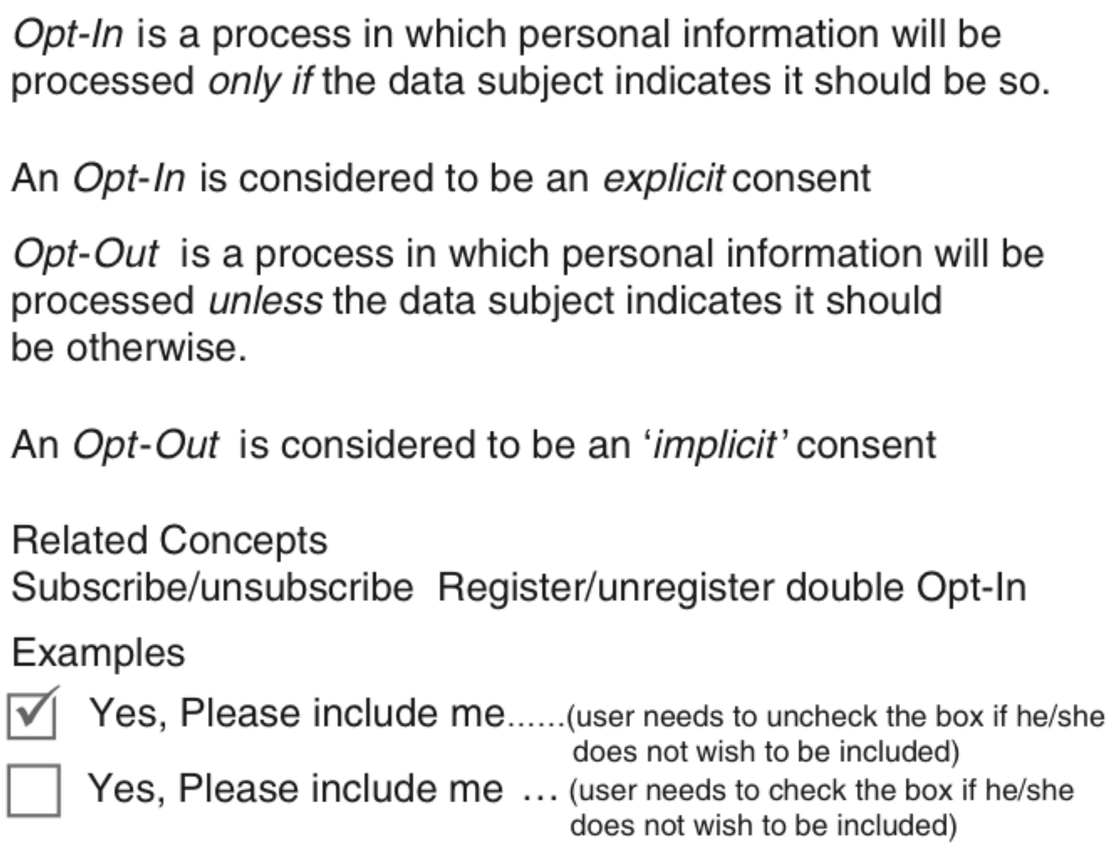

Figure 6.2 | Opt-In and Opt-Out.

believe that a *dynamic* IP address is NOT a PII because it varies depending on which computer network one is connected to, whereas a *static* IP address is a PII because it is always fixed. *Privacy notice* is considered as a mature privacy practice in organizations.

There are several protected disclosures to which the Model Bill's provisions relating to use and disclosure of PII do not apply. These non-applicability situations include the scenarios where the disclosure is made to service providers and related companies that operate under a common set of internal policies. The Model Bill also contains access and correction as well as security-related provisions, including a breach notification obligation. The breach notification is triggered when a security breach results in (or it is likely that a breach will result in) the misuse of a resident's unencrypted sensitive financial information. Table 6.2 shows alignment position of Asia-Pacific countries with regard to Microsoft's Model Privacy Bill as the benchmark.

According to Organization for Economic Co-operation and Development (OECD) "Guidelines on the Protection of Privacy and Trans-border Flows,"[10] the data protection laws in Australia, Hong Kong and New Zealand are moderately to favorably aligned with the benchmark legislation. The strengths of these regimes vis-à-vis the Model Bill include their broad application to the private sector and their notice, security and access provisions. There is one aspect of the Model Bill that these regimes have not adopted in full – it is the tiered consent model that takes account of the privacy risk inherent in secondary use or transfer (i.e., a model that imposes more onerous consent requirements where the associated privacy risk is greater). Furthermore, the imposition of restrictions on transborder data flows in Australia and Hong Kong are deviations from the Model Privacy Bill.

If we consider on its own, Japan's Act Concerning the Protection of Personal Information appears to be moderately aligned with the benchmark legislation. Yet, it is possible that the sectoral guidelines to explain the application of the Protection of Personal Information in certain industry sectors may alter this analysis. OECD Guidelines are used by South Korea's data protection regime as well; however, the South Korean data protection regime is less well aligned with the benchmark legislation. South Korea's alignment with the Model Privacy Bill is impacted by a combination of restrictive provisions in the legislation, such as requiring a data subject's consent for transborder data flows within a corporate group, and the way in which the legislation has been interpreted and enforced by the Korea Information and Security Agency (KISA).

Taiwan's Computer-Processed Personal Data Protection Law has limited applicability to certain industries in the private sector. The Taiwanese Law is unique in the region as long as it establishes a mandatory licensing regime for the regulated entities that collect, use or disclose personal data. Thailand does not have legislation for private sector data protection. However, the Official Information Act 1997 does regulate state agencies for dealings with personal information. Vietnam does not seem to have any comprehensive data protection laws of general application. However, the Vietenamese Law on Information Technology 2006 does contain a limited data protection provision applicable to the collection, use and disclosure of personal information in a networked environment. In the E-Transactions Law, there are similar provisions to address the handling of personal information collected as part of an electronic transaction – a very common phenomenon in E-Commerce paradigm. The Philippine Department of Trade and Industry has recently come out with an administrative order with guidelines to protect personal data held by private sector organizations. These voluntary guidelines are a measure of a different kind to the Model Bill; they aim at encouraging private sector organizations to adopt privacy policies rather than penalizing them for not doing so.

Malaysia (as at the time of writing this) does not have a comprehensive data protection legislation. However, the General Consumer Code developed following the Communications and Multimedia Act of 1998, contains provisions toward the protection of personal information collected by licensed telecommunications service providers. China, India, Indonesia and Singapore have not enacted data protection legislation per se. China, India, Indonesia, Malaysia, South Korea, Taiwan and Thailand are currently considering data protection legislation (as the time of writing this). APEC Privacy Framework in 2005 has served as the trigger for reform in this area.

The Taiwanese legislative proposal, when enacted, would bring the country's existing regime more into line with the ideal advocated by the benchmark legislation. The position in South Korea is not so clear; as at the date of writing this, it is understood that the South African Government has plans to consolidate three of their private sector instruments that were previously meant for consolidation into a single bill. The Indonesian and Indian data protection proposals are only minor parts of pending cybercrime legislation. Toward that, in September 2007, India's Standing Committee on IT recommended that India enact a more comprehensive data protection regime as part of the proposed amendments to the IT Act discussed in the computer security section previously.

For a long time, Malaysia, Thailand and China have been contemplating to have a legislation toward data protection. The most recent publicly available draft of the Malaysian legislation contemplated a model similar to Hong Kong's Personal Data Privacy Ordinance, which would stand the pending legislation in good stead vis-à-vis the Model Privacy Bill. It is understood that a further draft of Malaysia's data protection legislation has been prepared since then. The Thai Government is presently considering ways to come closer toward its proposed alignment with the APEC Privacy Framework. China's State Council Normalization Office is in discussions with data protection experts to finalize the content of their proposed legislation which was placed on the National People's Congress legislative agenda in 2008.

Spam Laws

The checklist drafted by Microsoft contains features of effective anti-Spam legislation. It is considered as the benchmark legislation for this part of the discussion. The Microsoft checklist envisages an "Opt-Out" anti-Spam regime to address commercial electronic messages. However, the checklist mentions that transactional or relationship messages (such as messages sent to customers with regard to products or services purchased from the sender) should be excluded from the scope of regulation, as it should contain messages that only have an incidental commercial purpose. The Microsoft checklist contains the usual restrictions on transmitting electronic messages of commercial nature – without an unsubscribe facility or accurate sender and header information – and provides that customers should be able to Opt-Out from the receipt of commercial electronic messages on a product-line basis as well as on a company-wide basis. However, the checklist does not contemplate any "ADV" or other labeling requirement. Effective anti-Spam legislation needs to also include strong antiaddress harvesting and dictionary attack measures, as well as service provider liability provisions that preserve the right of Internet Service Providers (ISPs) and E-Mail service providers to fight against Spam. As far as enforcement is concerned, the Microsoft checklist contemplates enforcement by ISPs, E-Mail service providers and the government. The available remedies should include: (a) civil liability in damages, (b) capped statutory damages that may be adjusted to take into account willful violations and implementation of best practice procedures and (c) criminal sanctions for intentional and unauthorized acts, including those involving fraud.

In recent times, there has been a discernible move in the Asia-Pacific region toward the enactment of anti-Spam legislation. There are now seven countries in this region that have enacted comprehensive anti-Spam legislation: Australia, China, Hong Kong, Japan, New Zealand, Singapore and South Korea. Of these, Hong Kong's Opt-Out regime appears to be the most closely aligned with the checklist, with Australia and New Zealand being positioned not too far behind despite implementing Opt-In models. Singapore has enacted an Opt-Out regime with "bulk" and labeling requirements, whereas the requirements of South Korea's regime vary depending on the medium by which the advertising is transmitted. China's Internet E-Mail Service Management Regulations 2006 are moderately to weakly aligned with the checklist due in part to their application only to E-Mails and their "AD" labeling requirement. Hong Kong and New Zealand are currently the only jurisdictions in the region that explicitly exclude transactional or relationship messages from the scope of regulation.

Philippines, Thailand and Vietnam have enforced anti-Spam measures that are less comprehensive. The broadcast messaging rules implemented in the Philippines are considered as an interim measure designed to address a particular area of concern, namely, Spam SMS and MMS, pending the development of a more comprehensive regime. Thailand chose to enact Spam-related provisions as part of its 2007 computer security legislation. Those provisions are likely to have limited application to Spam that is not fraudulent or designed to interfere with the operation of the recipient's computer system. Two sources of Spam-related obligations are available in Vietnam: (a) the Law on Information Technology 2006 and (b) Decree 142 Specifying Administrative Penalties in the Field of Post, Telecommunications and Radio Frequency. These instruments address "advertisement information" transmitted over networks and "unsolicited messages," respectively. However, neither instrument brings about a comprehensive Spam regime. In the absence of specific anti-Spam legislation, jurisdictions such as India, Indonesia, Malaysia and Taiwan rely on their existing computer security and/or consumer protection laws to regulate Spam activity. In a way, this approach succeeds toward eliminating the consequences of Spam activity; it is increasingly being accepted by legislatures in the region that specific anti-Spam legislation is necessary to reduce Spam volumes.

Legislatures in India, Indonesia, the Philippines and Taiwan are currently considering anti-Spam legislative proposals. Of these proposals, Taiwan's "Opt-Out" legislation appears to be the most advanced in the legislative process, as well as being the most closely aligned with the checklist (the meaning of the term "Opt-Out" has been explained earier; see Fig. 6.2). In India, the definition of *unsolicited commercial communications* is presently defined and is based on Opt-Out approach solicited by the Reserve Bank of India, that is, those customers who do not want to receive unsolicited commercial communications.

Vietnam's inter-agency taskforce is at an early stage of drafting a diktat on Spam. A draft of the diktat was expected in late 2007. The pending computer security laws in India, Indonesia and the Philippines contain Spam-related provisions. If enacted in their current form, the Spam-related provisions in India's IT Amendment Bill is to apply only to certain limited types of Spam and not mere unsolicited commercial electronic messages. In its report on the IT Amendment Bill, the Standing Committee on IT questioned whether these provisions contained a sufficient response to the problem of Spam. The Committtee recommended that India enact specific anti-Spam legislation.

Box 6.3 India and Anti-Spam Legislation

A few years ago, Bill Gates proclaimed that Spam would no longer be a problem in 2006. However it did not happen. Spam is nothing but unsolicited bulk E-Mail (UBE) or unsolicited commercial E-Mail (UCE). Note that Spam is "unsolicited" which means that there is no prior relationship between the parties concerned and the recipient has not explicitly consented to receive the communication. Unsolicited E-Mail, also called "Spam," is a growing concern among corporations and individuals. Spamming was once viewed as a mere nuisance – it is now posing alarming problems. Way back in 2002, losses to US Corporations due to Spamming were a staggering $8.9 billion. In 2003, Spam costs to all non-corporation Internet users were an estimated $255 million. With the increasing number of Internet users in India, the absence of any legislation prohibiting Spamming and the dearth of other Spam-control measures, it is time the government took note of this menace.

Spam legislation is non-existent in India. The ITA 2000 does not discuss the issue of Spamming at all. It only refers to punishment for those, who after having secured access to any electronic material without the consent of the person concerned, disclose such electronic material to any other person. It does not have any bearing on violation of individual's privacy in cyberspace. The illegality of Spamming is not considered. The Delhi High Court acknowledged the absence of appropriate legislation concerning Spam in a recent case wherein Tata Sons Ltd and its subsidiary Panatone Finwest Ltd filed a suit against McCoy Infosystems Pvt Ltd for transmission of Spam. It was held that in the absence of statutory protection to check Spam mails on Internet, the traditional tort law principles of trespass to goods as well as law of nuisance would have to be used.

Box 6.3 India and Anti-Spam . . . (*Continued*)

Spam is harmful because for a number of reasons as follows:

1. **Content:** Most of the objections to Spam come up due to its content. Commercial messages may promote dubious ventures; sometimes messages with sexually explicit material are commonplace. However, the most important objection to Spam messages is that they may contain harmful embedded code and hostile file attachments.
2. **Internet resources consumed:** A significant proportion of all E-Mail traffic constitutes of Spam, resulting in massive consumption of network bandwidth, memory, storage space and other resources. Internet users and system administrators spend a great deal of time reading, deleting, filtering and blocking Spam, as a result of which they pay more for Internet access.
3. **Threat to Internet security:** Spammers frequently tap into Simple Mail Transfer Protocol (SMTP) Servers and direct them to send copies of a message to a long list of recipients. Third-party relaying usually represents theft of service because it is an unauthorized appropriation of computing resources. A company's reputation may be damaged if it is associated with Spam because of third-party relaying.

The legal methods to deal with the Spamming menace are prohibition, enforcement of anti-Spam policies, Opt-Out clause, statutory provisions and enforcement mechanisms. Although there are legal methods to deal with Spam, there is considerable debate whether we need to prohibit or restrict Spam? Even if one assumes that Spam is bad, there are many countervailing issues that must be analyzed with regard to any legislation that prohibits or restricts Spam. These countervailing issues include the following:

1. Civil liberties advocates say that there are constitutional issues to consider which could trickle down to other types of speech over the Internet. Furthermore, different countries have different free speech laws. What may be legal in one country may be entirely unlawful elsewhere. In India, there are strong and explicit freedom of speech protections; the Supreme Court has held commercial advertising to be an inalienable part of freedom of speech which is enshrined in Article 19 of the Constitution. This is the reason why some legislators and advocates argue that the anti-Spam legislation has to be very specific in that the proposed legislation has to truly limit itself to only "commercial E-Mail."
2. Consumer protection laws exist to protect the consumer from fraudulent and deceptive advertising.
3. Legislation prohibiting pornography already exists although some modification to such legislation may be required, so that Internet users have some protection from receiving pornographic materials via Spam.

Indonesia's EIT Bill does not propose to regulate Spam messages per se. Instead, the EIT Bill proposes to require eSellers (i.e., persons who offer to sell goods and services offered through electronic media) to provide complete and correct information in relation to the terms of the contract, the good or service offered and the producer of the good or service. The Spam-related provisions in the Philippines' Cybercrime Prevention Act of 2005 (HB 3777) propose to establish a basic Opt-Out regime (refer to Fig. 6.2). Plans are afoot to amend Japan's law regarding the regulation of transmission of specific E-Mail. The Ministry of Internal Affairs and Communications was to submit a bill to the The National Diet of Japan (Japan's bicameral legislature) in 2008. The Bill was to create an Opt-In regime for Spam E-Mails accessed from computers and mobile phones. Malaysia and China may also enact anti-Spam laws in the future. There was an announcment in August 2007 by the Malaysian Communications and Multimedia Commission saying that it had issued a tender for the provision of consultancy services for studying legislative responses and drafting anti-Spam legislation for Malaysia. As for China, it is understood that the Internet Society of China, supported by the Ministry of Information Industry, is engaged in research to look into various possible approaches toward comprehensive Spam legislation. Draft codes of practice are under consideration in both Hong Kong and New Zealand. These codes of practice are expected to provide regulated entities with further guidance on how to comply with the comprehensive

Table 6.3 | Asia-Pacific region: Alignment of the countries enacted legislation with regard to anti-Spam laws (Microsoft checklist)

Favorable Alignment	*Moderate Alignment*	*Weak Alignment*
Hong Kong	Australia	India*
—	China	Indonesia*
—	New Zealand	Malaysia
—	Singapore	Philippines
—	South Korea	Taiwan*
—	—	Thailand
—	—	Vietnam

*No Spam laws have been enacted.

anti-Spam regimes that have recently been enacted in Hong Kong and New Zealand. Table 6.3 presents the alignment position of Asia-Pacific countries with regard to the Microsoft checklist for anti-Spam legislation.

Online Protection for Children

This is closely related to COPPA (refer to Chapter 1). For readers' reference, ICMEC stands for International Centre for Missing and Exploited Children. A combination of the child pornography offenses in Title 3 of the Convention on Cybercrime and the core elements of ICMEC's Model Child Pornography Legislation serve as the benchmark instrument for this part of the analysis. The child pornography offenses in Title 3 of the Convention of Cybercrime aim to circumscribe the use of computer systems in the commission of sexual offenses against children. As such, the Convention requires signatories to criminalize acts such as the production of child pornography for the purpose of its distribution through a computer system, and offering, making available, distributing or transmitting child pornography through a computer system. Being in possession of child pornography material in electronic form stored in a computer system is also subject to criminalization. In ICMEC's view, effective child pornography legislation must specifically apply to child pornography and not just pornography in general. Therefore, the legislation must include a definition of child pornography (where a child is a person under the age of 18 irrespective of the age at consent to sexual relations). In an effective child pornography, legislation should also expressly criminalize the possession of child pornography regardless of the intent to distribute, and require ISPs to bring to the notice of relevant authorities all suspected child pornography matters.

Online child safety laws are among the least developed in the region vis-à-vis the benchmark legislation. Most countries have enacted broad obscenity regimes that have some application to online dealing in child pornography. There are only 5 of 14 jurisdictions, namely, Australia, Hong Kong, Japan, South Korea and Taiwan, which have enacted legislation to specifically address child pornography. Three of the fourteen jurisdictions, that is, Australia, Hong Kong and Taiwan, have enacted legislation on computer-facilitated child pornography offenses. The specific child pornography legislation, enacted in the region, generally adheres to the applicable ICMEC principles; however, only Australia and Hong Kong criminalize mere possession of child pornography (i.e., possession, irrespective of the intent to distribute). The computer-facilitated child pornography offenses enacted in Australia, Hong Kong and Taiwan cover most of the prohibited acts under Title 3 of the Convention; Australia is the only jurisdiction in the region to impose an obligation on ISPs and content hosts to report material that they reasonably believe to be child pornography material (a similar provision exists in the US law). Although New Zealand has not enacted specific legislation to combat child pornography, case law confirms that New Zealand's classification regime does apply to child pornography, and certain of the offenses under that regime attract more serious sanctions where the offending publication

promotes sexual exploitation of children, among other things. The Thai Computer Crime Act criminalizes certain computer-facilitated dealings with pornography, it does not specifically refer to child pornography.

Although child pornography is now being touted as a global issue, there is no legislation in India, Indonesia, Malaysia, the Philippines, Singapore and Vietnam to specifically address child pornography. However, the absence of specific child pornography legislation in these countries needs to be understood in the context of these countries' approach to control pornographic content. For example, in some of the Asia-Pacific jurisdictions, such as Malaysia, Singapore and Vietnam, the ISPs are primarily held responsible for control of content as well as hosting of content. However, in Vietnam this responsibility lies with the state, society and schools. As such, these entities will be held responsible if obscene material is transmitted using their services. With this approach to control of content, the need for specific legislation to irradicate child pornography is not perceived as neccessary because it is believed that the approach serves to reduce the availability of child pornography online.

Currently, the Philippine, Indian, Indonesian and Japanese legislatures are considering online child safety laws. ITA 2008 addresses child pornography. Most of these pending laws are subsumed in the broader proposals to enact computer security laws. The Philippine legislation specifically applies to child pornography and not to pornography at large. In the Philippines, the enactment of the computer-facilitated child pornography offenses in the Cybercrime Prevention Act is a welcome development – inclusion of these online child pornographic offenses and the associated definitions are based on Title 3 of the Convention on Cybercrime. In Indonesia, the proposals to enact computer-facilitated pornography offenses are considered less comprehensive than the Philippine proposal. It is believed that the Indonesian propoals could benefit from further refinement to get them aligned with the benchmark legislation. Japan has pending computer security legislation; it includes offenses relating to the possession and distribution of obscene electronic records. The Japanese Government plans to amend the Law for Punishing Acts Related to Child Prostitution and Child Pornography, and for Protecting Children. The details of these planned amendments are not available at the date of writing. Way back in 2005, Thailand had considered amendments to its erstwhile online child safety laws, specifically in the area of child pornography. At this point of time, it is not known if or when this legislative proposal will proceed to enactment. As per recommendation of the Indian Standing Committee on IT, the Indian Government has revised the IT Amendment Bill in order to criminalize computer-facilitated dealings with child pornography in accordance with the Convention on Cybercrime. With regard to *online child safety*, the Internet Governance Forum (IGF) is one of the active forums. Table 6.4 shows alignment position of Asia-Pacific countries with regard to Online Child Safety Legislation.

Table 6.4 | Asia-Pacific region: Alignment of the countries enacted legislation with regard to European Cybercrime Convention and ICMEC's Model Child Pornography Legislation

Favorable Alignment	*Moderate Alignment*	*Weak Alignment*
Australia	Hong Kong	India*
—	Japan	Indonesia*
—	South Korea	Malaysia
—	Taiwan	New Zealand
—	—	Philippines
—	—	Singapore*
—	—	Thailand
—	—	Vietnam*

*No online child safety laws have been enacted.

Let us consider three important geographies – Asia-Pacific, Europe (where privacy and security laws are very strictly laid out) and the US (where they have chosen a sector-based approach to information security). Positions in these geographies do differ. For example, in the US, there are state laws for prevention of cybercrime. Readers may visit the link given in Ref. #17, Additional Useful Web References, Further Reading which is about US Laws and Legislation. The US Federal Trade Commission estimates that identity theft affects 9 million Americans annually. The US Congress, in September 2008, passed a crack down on cybercrime after adding an amendment containing most of an anti-Spyware bill. This is further discussed in the following section. To conclude the discussion in this section, we note that the world scenario on legal position on cybercrime differs.

6.2.3 Anti-Spam Laws in Canada

In early 2009, the Canadian Government tabled anti-Spam legislation, Bill C-27, The Electronic Commerce Protection Act, to address Spam, counterfeit websites and Spyware. The proposed legislation also brings amendment to Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA – see Box 6.4) which covers online privacy in detail and contains many provisions relevant to E-Mail marketing.

Box 6.4 PIPEDA – The Canadian Act for Protecting Personal Information

Canada has two federal privacy laws, the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The Privacy Act took effect on 1 July 1983. This Act imposes obligations on some 250 Federal Government departments and agencies to respect privacy rights by limiting the collection, use and disclosure of personal information. It gives individuals the right to access and request correction of personal information about themselves held by these Federal Government Organizations.

Individuals are also protected by the PIPEDA that sets out ground rules for how private sector organizations may collect, use or disclose personal information in the course of commercial activities. The law gives individuals the right to access and request correction of the personal information these organizations may have collected about them. Initially, PIPEDA applied only to personal information about customers or employees that was collected, used or disclosed in the course of commercial activities by the federally regulated private sector, organizations such as banks, airlines and telecommunications companies. The Act now applies to personal information collected, used or disclosed by the retail sector, publishing companies, the service industry, manufacturers and other provincially regulated organizations. The Act does not apply to the personal information of employees of these provincially regulated organizations.

Basically, PIPEDA is based on the FIPs (Fair Information Practices):

1. Principle 1 – Accountability
2. Principle 2 – Identifying purposes
3. Principle 3 – Consent
4. Principle 4 – Limiting collection
5. Principle 5 – Limiting use, disclosure and retention
6. Principle 6 – Accuracy
7. Principle 7 – Safeguards
8. Principle 8 – Openness
9. Principle 9 – Individual access
10. Principle 10 – Challenging compliance

For more information, contact
The Office of the Privacy Commissioner of Canada
112 Kent Street, Ottawa, ON K1A 1H3
www.priv.gc.ca
1-800-282-1376

Note: The PIPEDA and the FIPs are also addressed in Chapter 29 and Appendix H, respectively, in Nina Godbole (2009) *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

There are two laws currently being discussed in Canadian legislative assemblies:

1. **Senate Bill S-220:** The bill was introduced by Senator Yoine Goldstein in early February 2009. It is slated to become the *Anti-Spam Act*. It is a private member's bill with private right of action and criminal remedies. Senator Goldstein has already introduced the Anti-Spam Bill in two previous sessions of parliament. The purpose of this bill is to ban UCE. Bill S-220 replaces the Canadian Bill S-202 (see Ref. #20, Additional Useful Web References, Further Reading). The bill would allow the ISPs to refuse, filter and block Spam E-Mails. The S-220 is proposing to consider Phishing attacks also. According to some legislative experts, there could be potential conflicts between the problematic parts of this proposed legislation and the Canadian Charter of Rights and Freedoms. These conflicts are being looked into because it is felt that it would be a simplify justification for removing sections that contain exemption to spamming (Section 8, subsection 3, paragraphs a, b, c, d and g). The motive for this bill is based on the fact that despite the widespread recognition that Spam is a serious problem which costs our economy billions in fraud and lost productivity, Canada remains the only G8 country without an anti-Spam legislation.
2. **Parliamentary Bill C-27:** The bill was tabled by the government in April 2009, with private right of action, coordination between various enforcement agencies, civil remedies. The Electronic Commerce Protection Act (ECPA) (aka: Bill C-27) is an Anti-Spam Act that covers *E-Mail communications, unauthorized installed applications* and the *alteration of data during transmission between senders and recipients*. The bill forbids anyone from installing a program on a computer that could send an electronic message without the consent of the owner or user. It also forbids anyone in Canada from sending a commercial message to any electronic address unless the receiver has consented. An exception is if the person sending the message has had a business transaction with the recipient in the previous 18 months. Penalties range from up to $1 million for individual violators to up to $10 million for organizations. One of the criticisms against the bill is that "the bill as currently drafted would actually ban the use of the Internet by Canadians unless a person with a website had written consent from a consumer to use it." Instead of demanding consent for certain activities, Ottawa needs to define activity that is bad – for example, creating misleading E-Mail headers.

Box 6.5 ECPA: The New Dawn in Canadian Legislation

The Electronic Commerce Protection Act (ECPA) is a law designed to promote and protect electronic communications while discouraging the abuse of these resources that threaten to impair the reliability, efficiency of electronic activities; prevent additional costs to businesses and consumers; protect the privacy and the security of confidential information and strengthen the confidence of Canadians in the use of electronic means of communication and commercial activities. This enactment also makes several amendments to related laws; the Competition Act, PIPEDA, the Canadian Radiotelevision and Telecommunications Commission Act, and the Telecommunications Act.

The ECPA defines a commercial electronic message as an electronic message that consists of: (a) the content, (b) the hyperlinks and (c) the contact information, where the purpose is to encourage participation in a commercial activity that:

1. Offers to purchase, sell, barter or lease a product, goods, a service, land or an interest or right in land;
2. offers to provide a business, investment or gaming opportunity;
3. advertises or promotes anything referred to in (1) or (2);
4. promotes a person, including the public image of a person, as being a person who does anything referred to in any of (1)–(3), or who intends to do so.

Box 6.5 ECPA: . . . (*Continued*)

The ECPA also clearly states that an electronic message which contains a request for consent (i.e., confirmed Opt-In notices) is also considered to be a commercial electronic message. The ECPA also lists several types of excluded communications such as responses to customers' service enquiries and applications, law enforcement, public safety, the protection of Canada, the conduct of international affairs or the defense of Canada and personal communications.

The governance ambit of ECPA looks very large in the sense, which after reading through the act, it looks like every corporation registered under a Federal or Provincial license for the purposes of Commercial Activity is going to be effected by this law. This covers non-profits, co-ops, sole proprietors and partnerships. The Communications Assistance for Law Enforcement Act (CALEA) is the Amendment of ECPA.

Commercial E-Mail can only be send to a recipient who has consented to receiving it (express or implied – definition below) and the message complies with the purpose of the ECPA described above. All messages being sent must:

1. Clearly identify the person who sent the message and the person (if different) on whose behalf it is sent – *Add your physical postal address and company name to all E-Mails*.
2. Provide a method where the recipient can readily contact the person(s) responsible for sending the message (MUST be active for 60 days after the messages was sent) – *Enable replies to go to your customer service and stop using No-Reply*.
3. Provide a working unsubscribe mechanism (more below) that removes an address within 10 days – *The faster the better.*

An important point to note is that the ECPA states that an electronic message is considered to have been sent once its transmission has been initiated (by the sender) and that it is irrelevant if the intended recipient address exists or if message reaches its intended destination. This reference makes bounce management even more important for mailers to monitor and clean from your list. When you are working with your clients/members/subscribers and asking for their consent, there are several things you should remember and incorporate into the process:

1. Clearly state the purpose(s) for which the consent is being sought.
2. Clearly identify the person(s) seeking consent.
3. Clearly define any other prescribed information about how data is collected and plans to be used.

There are significant monetary penalties that have been set out within the Act. The maximum penalty for a violation is $1,000,000 in the case of an individual, and $10,000,000 in the case of any other person.

For more details on ECPA refer to the link http://blog.deliverability.com/2009/04/canadas-electronic-commerce-protection-act.html (19 August 2009).

6.2.4 Cybercrime and Federal Laws in the US

On 15 September 2008, the US House of Representatives approved the bill H.R. 5938. The amendment, as part of Senate Bill S. 2168, was meant to expand the ability of the Federal Government to prosecute criminal of identity theft and to allow victims to seek compensation for the victims' efforts (time and money) spent on trying to restore their credit. The legislation was signed by President George W. Bush. It had provisions for a fine as well as imprisonment up to 5 years for Spyware. It is believed that this amendment closes the gap on existing identity theft laws which originally only allowed federal prosecution under the scenario that the perpetrator used interstate or foreign communications to access a computer. The only exception were cases involving Federal Government computers or financial institutions. With President's action of signing the bill into Law, Federal prosecutors will be empowered to pursue cases having the perpetrator and victim from the same jurisdiction.

The amendment puts a criminal penalty on the use of malicious Spyware and that of keystroke loggers with the intent of damaging a computer. Furthermore, the amendment eliminates the requirement that the loss must exceed $5,000, thus, making it a bad behavior to send Spyware that causes any loss. Accused criminals (when proved guilty) will need to pay fine as well as face imprisonment up to 1 year. The legislation would make it an offense to use Spyware or keystroke loggers to damage computers and as such there will be up to 10 years imprisonment. With this bill, it is considered a crime to obtain, delete or release data from a computer or to threaten to crash a computer/computer system. With this bill set, cyberextortion is criminalized by making it a criminal offense to demand money with regard to a protected computer. Those who violate this would end up in prison for a period up to 5 years for the first offense and up to 10 years for the second offense. The bill also adds a conspiracy charge to cybercrime laws and allows confiscation of property/equipment/means used to commit cybercrimes. To understand Computer Crime & Intellectual Property Section of the United States Department of Justice visit [9] in References section.

Box 6.6 The Florida Computer Crimes Act

Unauthorized use of computing facilities is a crime under the Florida Computer Crimes Act. The Act provides definitions to the various terms related to computer crime: *Offenses against intellectual property, offenses against computer equipment or supplies* and *offenses against computer users*.

The full text of the Florida Computer Crimes Act (1988 version) and a summary of the penalties referenced in the Act are available in the document accessible at the link mentioned at the end of this Box.

The Act specifies the following type of crimes:

1. Offenses against intellectual property;
2. offenses against computer equipment or supplies;
3. offenses against computer users.

- *Computer program* means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data. It means an internally programmed, automatic device that performs data processing.
- *Computer software* means a set of computer programs, procedures and associated documentation concerned with the operation of a computer system.
- *Computer system* means a set of related, connected or unconnected computer equipment, devices or computer software.
- *Computer network* means a set of related, remotely connected devices and communication facilities including more than one computer system with the capability to transmit data among them through communication facilities.
- *Computer system services* means providing a computer system or computer network to perform useful work.
- *Property* means anything of value as defined in S.812.011 and includes, but is not limited to, financial instruments, information including electronically produced data and computer software and programs in either machine or human-readable form, and any other tangible or intangible item of value.
- *Intellectual property* means data, including programs.
- *Instrument* means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card or marketable security.
- *Access* means to approach, instruct, communicate with, store data, retrieve data or otherwise make use of any resources of a computer, computer system or computer network.

The Act also defines felony of first, second and third degree. The full text of the Florida Computer Crimes Act (1988 version) and a summary of the penalties as per this Act can be accessed at the following link:
http://docweb.cns.ufl.edu/docs/d0010/d0010.pdf

For further details on this act, please refer to the following link:
http://www.clas.ufl.edu/docs/flcrimes/chapter2_1.html (5 December 2009).

6.2.5 The EU Legal Framework for Information Privacy to Prevent Cybercrime

The EU is an economic and political union of 27 member states, located primarily in Europe. Readers can visit the link to understand the EU member countries.[4] Also see Box 6.7 to know the names of EU member countries. Data protection EU legal framework addressed the principles for information management (fairness, consent, transparency, purpose specification, data retention, security and access). The right to privacy is a highly developed area of law in Europe. All the member states of the EU are also signatories of the European Convention on Human Rights (ECHR). The EU believes that law is the enabler for trust and confidence in the Information Society. However, law is not self-acting; personal data is disclosed by default; online anonymity does not have same status as physical and identification is considered critical for combating crime. However, technology is required to assist in compliance and enforcement. As the global "Information Age" continues to evolve, international understanding of the policy options for data protection also evolves, guided by an understanding of the practical consequences and effectiveness of such laws.

There is a Data Protection Directive (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) known as the EU directive which regulates the processing of personal data within the EU. It is considered as the most important component of EU privacy and human rights law. In 1995, the European Commission implemented the EU directive.

In the EU, cybercrime law is primarily based on the CoE's Convention on Cybercrime (November 2001). Under the convention, member states are obliged to criminalize:

1. Illegal access to computer system (see Box 6.1);
2. illegal interception of data to a computer system;
3. interfering with computer system without rights and intentional interference with computer data without rights;

Box 6.7 The EU Member Countries

The European Union (known as the EU) was formed in 1951. At the time of writing this, there are 27 countries that are member of the EU:

1. UK	8. Italy	15. Austria	22. Luxembourg
2. France	9. Netherlands	16. Belgium	23. Estonia
3. Germany	10. Hungary	17. Cyprus	24. Slovakia
4. Denmark	11. Ireland	18. Romania	25. Slovenia
5. Sweden	12. Poland	19. Bulgaria	26. Latvia
6. Finland	13. Portugal	20. The Czech Republic	27. Lithuania
7. Greece	14. Spain	21. Malta	

Bulgaria and Romania are the most recent member states; they joinied the EU on 1 January 2007. Other states are also trying to join and negotiations are in progress with them. Figure 6.3 shows the relationships between various supranational European organizations (courtesy Wikipedia). The term *supranational union* implies a supranational political entity that lies somewhere between a "confederation," that is, an association of states and a federation that is a state.

Note: The mention of CoE is referred to, after Box 6.8, in the context of cybercrime legislation.

Box 6.7 The EU . . . (*Continued*)

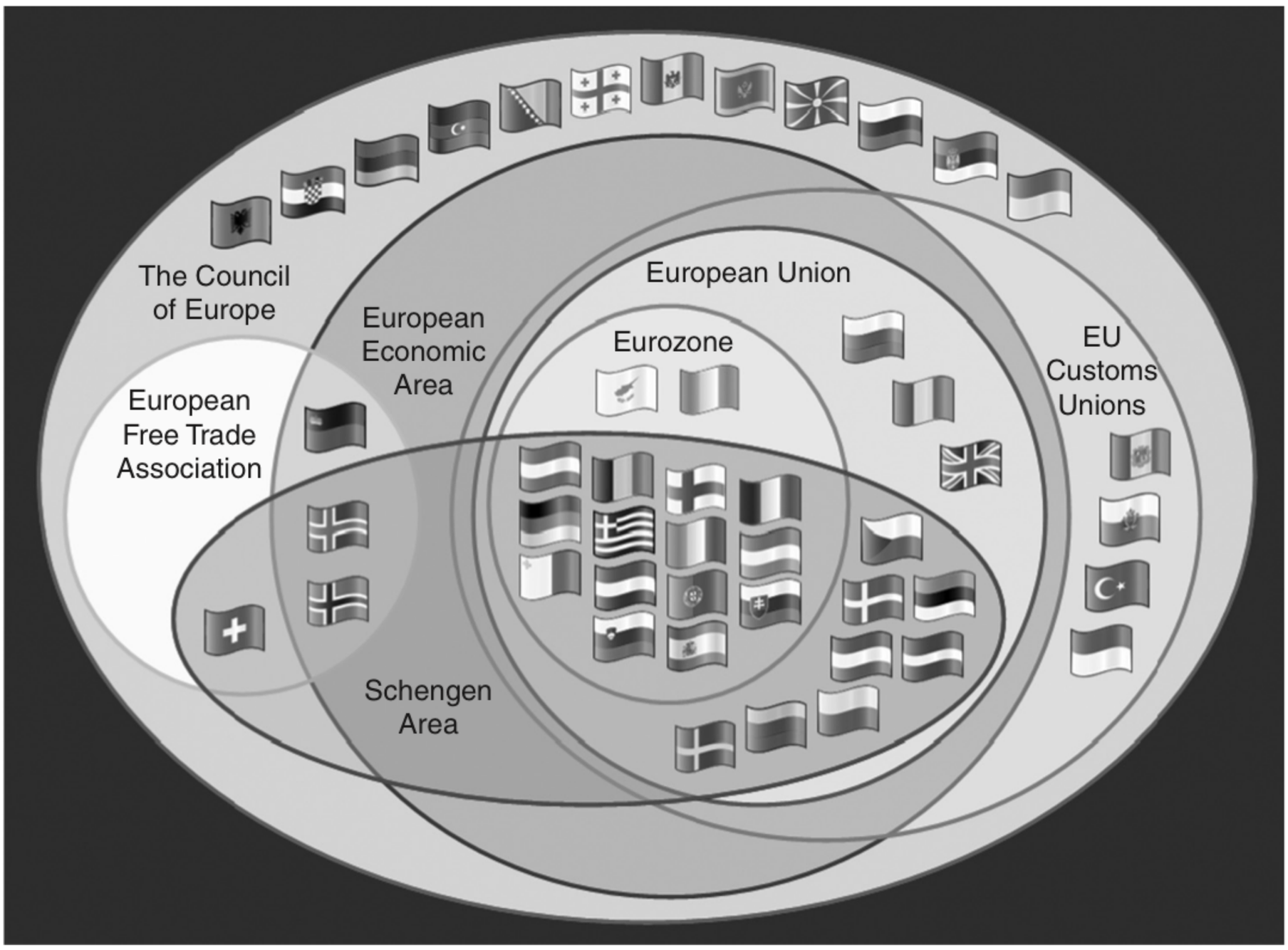

Figure 6.3 Relationships among supranational European organizations.
Note: The color version of the figure is available in CD.

4. the use of inauthentic data with intent to put it across as authentic (data forgery);
5. infringement of copyright-related rights online;
6. interference with data or functioning of computer system;
7. child pornography-related offenses possession/distribution/procuring/producing of child pornographic (recall the discussion in Chapter 1 about COPPA).

Box 6.8 The European Data Protection Directive

Under the EU directive, member states are under obligation to do the following:

1. To ensure that data is processed fairly and lawfully and that it is collected for specified and legitimate purposes and not processed in a manner incompatible with those purposes.
2. The processing of data is adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed.
3. The data collected is accurate and kept up to date and in a form which permits identification of data subjects.

Box 6.8 The European . . . (*Continued*)

4. Personal data may be processed only if:
   - The data subject has unambiguously given his consent;
   - processing is necessary for the performance of a contract to which the data subject is party;
   - processing is necessary for compliance with a legal obligation;
   - processing is necessary in order to protect the interests of the data subject;
   - processing is necessary for the performance of a task carried out in the public interest, etc.
5. The directive prohibits the processing of certain personal data such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, health or sex life or processing for the purposes of preventive medicine, medical diagnosis, offenses and criminal convictions, etc. except under certain conditions.
6. To provide to the data subject certain information such as identity of the entity processing the data, purposes of the processing, recipients of the data, etc.
7. If the data was not obtained from the data subject, member states are to provide that the entity processing the data must provide the data subject with information such as identity of the entity, purposes of processing, categories and recipients of data, etc.
8. To provide the right to access the data to the data subjects without constraint at reasonable intervals.
9. The data subject must be provided a right to object to the processing of data relating to him and where there is a justified objection, it must be provided that the processing may no longer involve the data.
10. Apart from imposing an obligation to keep the confidentiality of processing of data, the entity processing the data must be required to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, accidental loss, unauthorised disclosure, etc.
11. The transfer of personal data to third countries by member states must be done only under certain conditions.

The Data Protection Directive, therefore, covers a whole range of issues associated with processing of personal data in keeping with the twin objectives of the Directive.

In principle, there are similarities between the US regulation and law enforcement of cybercrime in the EU. Cyberfraud (this term is explained in Chapter 1) and making intentional false representations online (that victims rely on) is a federal offense in the US. Identity theft that takes place in the form of unauthorized use of another person's SSN, driver's license, work ID or credit card online is also a federal cybercrime. ID Theft is addressed in Chapter 5.

6.2.6 Cybercrime Legislation in the African Region

There is a common agreement that the African regions are in dire need for legislation to fight cybercrime. Africa is witnessing explosive growth in ICTs. With this growth, however, cybercrime has also become a reality in this part of the world too. African countries, mostly because of inadequate action and controls to protect computers and networks, are targets of attack. A great deal of criminal activity is said to take place from this part of the world. We heard about the Nigerian 419 scam (more on this is discussed in Section 11.7.19, Chapter 11 in CD) or the story of the young Zambian who hacked into a government website and replaced the picture of the erstwhile president Frederick Chiluba with a cartoon! In early 2008, a good number of South African banks became victims of Phishing attacks (Chapter 5 addresses Phishing attacks).

Box 6.9 The European Convention on Cybercrime

In 1997, there was the meeting of experts and the CoE formed a Committee on Crime in Cyberspace. The experts kept meeting in a clandestine fashion for several years. Ultimately, they succeeded in drafting an international treaty entitled the *Convention on Cybercrime* known as "the Convention." Finally it was released in June 2001. The Convention on Cybercrime is the first international treaty seeking to address cybercrime and Internet crimes by harmonizing national laws, improving investigative techniques and increasing cooperation among nations. It was drawn up by the CoE in Strasbourg with the active participation of the CoE's observer states Canada, Japan and the USA. Of the 34 countries that participated in the ceremonial act of signing the Convention in November 2001, only 6 countries have actually ratified the Convention. No major European country has agreed to be bound by the Convention. The only countries that have ratified it are Albania, Croatia, Estonia, Hungary, Lithuania and Romania.

The main aim of the Convention is to pursue "a common criminal policy aimed at the protection of society against cybercrime, *inter alia* by adopting appropriate legislation and fostering international cooperation." The Convention includes a list of crimes that each signatory state must transpose into their own law. It requires the criminalization of such activities as hacking (including the production, sale or distribution of hacking tools) and offenses relating to child pornography, and expands criminal liability for intellectual property violations. It also requires each signatory state to implement certain procedural mechanisms within their laws. For example, law enforcement authorities must be granted the power to compel an ISP to monitor a person's activities online in real time. Finally, the Convention requires signatory states to provide international cooperation to the "widest extent possible" for investigations and proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense. Law enforcement agencies will have to assist police from other participating countries to cooperate with their "mutual assistance requests."

In a significant development of March 2009, the CoE has asked India to be a part of its Convention on Cybercrime. This will lead to efficient cooperation with other 47-member countries, whenever such crimes are committed in India.

Credit card-related frauds are on the rise in the continent, especially in Egypt, South Africa, Kenya, Ghana and Nigeria, with losses estimated in billions of US dollars. E-Mail scams seem to be an African specialty, with West African countries among the major perpetrators. In Section 11.4.2 of Chapter 11, there are several illustrations provided on credit card-related frauds.

Some members of the African Union (Mauritius, South Africa and Zambia) have adopted cybercrime legislation. For example, in Botswana, cybercrime bill passed the second reading in the Parliament in December 2007. The bill is expected to go for third reading in the near future before it is signed into law. A draft Information and Communications Bill 2008 has been introduced in Gambia. The bill includes provisions on computer misuse and cybercrime issues. The East Africa region includes Tanzania, Kenya and Uganda. The progress on cybercrime legislation has been slow in this region, except for Uganda. The Computer Misuse Bill was introduced in 2008 in Uganda and a legislative process has started. The East African countries are trying to coordinate efforts so that the legislations should be similar to the cybercrime laws in the Southern African region. A Cybercrime Bill was prepared in Algeria for submitting it to the Parliament by the end of 2008; this is as per information mentioned on the link http://www.magharebia.com/cocoon/awi/xhtml1/en_GB/features/awi/reportage/2008/05/16/reportage-01. Latest update on the Algerian cybercrime bill position may be found at the link: http://apex.apkn.org/apex-in-detail/information-society-in-africa/algeria (28 October 2010).

Overall, it looks like the process of strengthening of legislation has been initiated in a large number of African countries, however, the process is rather slow and sometimes incoherent, and not necessarily taking into account international standards. Although there are exceptions and challenges in the African region, the ability of most African countries to investigate, prosecute and adjudicate cybercrime and cooperate internationally is limited. There is a serious risk that African countries develop legislation that is not compatible or harmonized with that of other countries, in particular that of countries providing servers and services with which cooperation would be most necessary. During the period September 2006–February 2009, Economic Crime Division of the Directorate General of Human Rights and Legal Affairs took up a cybercrime project. At the end of that project, they submitted their final report according to which the legislative scenario in some of the African countries emerges to be as presented in Table 6.5.

Table 6.5 | Cybercrime legislation in some of the African countries

Name of the African Countries	*Recommendation on Cybercrime Legislation*
Nigeria	There are several acts in force. They cover several aspects of cybercrime. A draft law on cybercrime is before the Parliament. The draft was expecting CoE review to elicit their support to bring it fully in line with the Convention. An analysis of the draft has been provided by the CoE in January 2008.
Ghana	A draft bill on cybercrime is available but needs a review to validate against the provision of the Convention. Accession to the Convention should be considered in the future.
Togo	There is no specific legislation in place. A working group needs to be established to develop a law on cybercrime in line with the Convention.
Niger	There is a package of laws prepared to provide a legal framework for information and communication technologies. The package has been submitted and is before the Parliament. This package expects deep analysis by the CoE. Accession to the Convention on cybercrime should also be considered.
Mali	Currently, no legislation is available. A national law on cybercrime is expected to be developed along the lines of international standards such as the Convention on Cybercrime.
Benin	Draft amendments to the criminal code and criminal procedure code are presented to the Parliament. It is recommended that relevant provisions should be reviewed to take into account the Convention on Cybercrime's views.
Congo	Currently, no legislation is available; however, review of criminal code and criminal procedure code is underway. It was recommended that a working group be established to develop a specific law on cybercrime in line with the Convention with the support of the CoE. Accession to the Convention should be considered once the law is in place.

Source: The Report by the Economic Crime Division of the Directorate General of Human Rights and Legal Affairs, Cybercrime project run during the period September 2006–February 2009).

Note: For CoE Convention on Cybercrime frequently asked questions and answers, visit the link at http://www.cybercrime.gov/COEFAQs.htm (24 August 2009). To get an idea about the location of the countries in the African continent given in the table, readers can consult the country-wise map of Africa. One such map can be accessed at the following URL: http://www.africaguide.com/afmap.htm

In South Africa "peace and security" is recognized as the essential human right. South Africa acknowledges peace and security to be fundamental and intrinsic to the democratic right for its citizens. South Africa being one of the most developed and prosperous economies in the African region, we must understand the legislative position of South Africa about cyberlaws. The discussion in this subsection is with that intent. During 13 November 2008 speech in Geneva at the high-level segment of the ITU Council, Radhakrishna L Padayachie, Deputy Minister of Communications, Republic of South Africa, addressed two issues related to the building of confidence and security in the use of ICTs, namely,

1. The measures that are in place and planned by the Republic of South Africa to enhance cooperation and collaboration on cybersecurity with other stakeholders at the regional, national and global levels and
2. the main challenges that should be tackled to ensure that the information society is safer and more secure at the global level.

In general, however, South African law does not prohibit unwelcome advertising. Advertising by the marketing communications industry is regulated by the Advertising Standards Authority of South Africa. In addition to this, South Africa has also got legislation governing "Spam." In July 2009, South African President assented to the *Electronic Communications and Transactions Act* (ECT Act) 2002. The purpose of the ECT Act is

> *"to provide for the facilitation and regulation of electronic communications and transactions; to provide for the development of a national e-Strategy for the Republic; to promote universal access to electronic transactions; to provide for human resource development in electronic transactions; to prevent abuse of information systems; to encourage the use of E-government services; and to provide for matters connected there-with."*

The material in this Act is divided into 14 chapters – among them are Chapter 7 is about Consumer Protection, Chapter 8 is about Protection of Personal Information and Chapter 13 is about Cybercrime.

In South Africa, the Department of Communications is mandated by the Electronic Communications and Transaction Act 2002, among others, to deal with cybercrime and other cybersecurity-related issues:

1. As far as identity management is concerned, the South African Accreditation Authority (SAAA) is responsible for accreditation of authentication services and products and more importantly the accreditation of service providers who will issue advanced digital signatures. This is for the purposes of ensuring business efficiency, quality of services, information security, and privacy and consumer trust in online transactions.
2. For cryptography, South African legislation provides for the registration of the cryptograph service providers with the Department of Communications.
3. South African legislation has the provision for the establishment of a cyberinspectorate, among others, to ensure compliance of cryptography service providers, authentication service providers and critical database management.

In line with the key cybersecurity focus areas developed by the GCA (*G*lobal *C*ybersecurity *A*genda of the ITU – International Telecommunication Union), the planned framework in South Africa will, among others, encompass the following key features:

1. **Legal measures:** In view of the borderless nature of cyberspace, our national laws that currently address the threat of cybercrime may have to be evaluated against the international best practices envisaged

in the model cybercrime legislation that is recommended as globally applicable and interoperable. This work will necessitate reviewing our existing national laws that deal with cybercrimes.

2. **Technical and procedural measures:** The emphasis will be on providing key measures to promote the adoption of enhanced approaches to improve security and risk management in cyberspace. The Republic of South Africa is working toward establishing Computer Security Incident Response Teams (CSIRTs) under the auspices of the Electronic Communication Security (Pty) Ltd (COMSEC). South Africa is also collaborating with some countries with a view to become a member of the Forum for Incident Response and Security Teams (FIRSTs).

As part of South Africa's determination to collaborate on cybersecurity with other stakeholders at the regional, national and global levels, South Africa has joined the Southern Africa Development Community (SADC) that consists of 14 African countries. SADC countries are on track to harmonize their Internet laws to effectively deal with computer-related crimes, and have finalized legislation for fighting cybercrime. It is said that all the SADC countries have agreed to alter parts of their cybercrime laws and come up with common rules.

For greater details about what the ECT Act of South Africa states about Spam filters, readers are advised to visit Ref. #23, Additional Useful Web References, Further Reading. Having taken an overview of the world legislative picture, now we come to India-specific discussion with focus on the IT Act and its amendments.

6.3 Why Do We Need Cyberlaws: The Indian Context

Cyberlaw is a framework created to give legal recognition to all risks arising out of the usage of computers and computer networks. Under the purview of cyberlaw, there are several aspects, such as, *intellectual property*, *data protection and privacy*, *freedom of expression* and *crimes committed using computers*. The Indian Parliament passed its first cyberlaw, the ITA 2000, aimed at providing the legal infrastructure for E-Commerce in India. ITA 2000 received the assent of the President of India and it has now become the law of the land in India. The Government of India felt the need to enact relevant cyberlaws to regulate Internet-based computer-related transactions in India. It manages all aspects, issues, legal consequences and conflict in the world of cyberspace, Internet or WWW. In the Preamble to the Indian ITA 2000, it is mentioned that it is an act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as *electronic commerce*. The reasons for enactment of cyberlaws in India are summarized below:

1. Although India possesses a very well-defined legal system, covering all possible situations and cases that have occurred or might take place in future, the country lacks in many aspects when it comes to newly developed Internet technology. It is essential to address this gap through a suitable law given the increasing use of Internet and other computer technologies in India.
2. There is a need to have some legal recognition to the Internet as it is one of the most dominating sources of carrying out business in today's world.
3. With the growth of the Internet, a new concept called *cyberterrorism* came into existence. Cyberterrorism includes the use of disruptive activities with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives in the world of cyberspace. It actually is about committing an old offense but in an innovative way.

Keeping all these factors into consideration, Indian Parliament passed the Information Technology Bill on 17 May 2000, known as the ITA 2000. This law is based on Model UNCITRAL law for E-Commerce (see Ref. #11, Articles and Research Papers, Further Reading). It talks about cyberlaws and forms the legal framework for electronic records and other activities done by electronic means. There are strengths as well as limitations in the ITA 2000; they are explained in Sections 6.4.2 and 6.4.3. A legal framework for the cyberworld was conceived in India, in the form of a draft E-Commerce Act 1998 – thereafter, the subject of cyberlaws started haunting the government. The basic law for the cyberspace transactions in India has emerged in the form of the ITA 2000. With that background, the Indian IT Act is briefly discussed in the following section.

6.4 The Indian IT Act

As mentioned above, this Act was published in the year 2000 with the purpose of providing legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as *electronic commerce*. Electronic communications involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the government agencies. Another purpose of the Indian IT Act was to amend the Indian Penal Code (IPC),[11] the Indian Evidence Act 1872,[12] the Bankers' Books Evidence Act 1891,[13] the Reserve Bank of India Act 1934[14] and matters connected therewith or incidental thereto. Cybercrimes punishable under various Indian laws are mentioned in Box 6.10. The Reserve Bank of India Act has got Section 58B about Penalties. Subsequently, the Indian IT Act underwent some important changes to accommodate the current cybercrime scenario; a summary of those changes is presented in Table 6.7 – note specially the changes to Section 66 and the corresponding punishments for cyberoffenses. Readers should also refer to Section 6.8.1 (Overview of Changes Made to the Indian IT Act) where the changes are explained in details.

Box 6.10 Cybercrimes and Other Related Crimes Punishable under Indian Laws

1. Under Section 65 of *Indian Copyright Act* any person who knowingly makes, or has in his/her possession, any plate for the purpose of making infringing copies of any work in which Copyright subsists is punishable with imprisonment which may extend to 2 years with fine.
2. Sending pornographic or obscene E-Mails are punishable under *Section 67 of the IT Act*.
   - An offense under this section is punishable on first conviction with imprisonment for a term, which may extend to 5 years and with fine, which may extend to 1 lakh rupees (₹ 100,000).
   - In the event of a second or subsequent conviction, the recommended punishment is imprisonment for a term, which may extend to 10 years and also with fine which may extend to 2 lakh rupees (₹ 2,00,000).
3. E-Mails that are defamatory in nature are punishable under *Section 500 of the Indian Penal Code* (IPC) that recommends an imprisonment of upto 2 years or a fine or both.
4. Threatening E-Mails are punishable under the provisions of the IPC pertaining to criminal intimidation, insult and annoyance (CHAPTER XXII) and extortion (CHAPTER XVII).
5. E-Mail spoofing is covered under provisions of the IPC with regard to fraud, cheating by personation (CHAPTER XVII) and forgery (CHAPTER XVIII).

The scope and coverage of the Indian IT Act is briefly described in Section 27.4, Ref. #6, Books, Further Reading. The structure of the Indian ITA 2000 is provided in Table 6.6 for readers' immediate reference. The sections mentioned in bold italics are relevant in the discussion of cybercrime and information security.

Table 6.6 | The Indian ITA 2000: Summary of contents (main elements only)

Chapter Number	*Chapter Title*	*Names of the Sections in the Chapter*
CHAPTER I	*Preliminary*	1. Short title, extent, commencement and applications 2. Definitions of key terms mentioned in the Act
CHAPTER II	*Digital Signature and Electronic Signature*	3. Authentication of electronic records
CHAPTER III	*Electronic Governance*	4. Legal recognition of electronic records 5. Legal recognition of electronic signatures 6. Use of electronic records and digital signatures in government and its agencies 7. Retention of electronic records 8. Publication of rule, regulation, etc., in Electronic Gazette 9. Sections 6, 7 and 8 not to confer right to insist document should be accepted in an electronic form 10. Power to make rules by Central Government in respect of digital signature
CHAPTER IV	*Attribution, Acknowledgment and Despatch of Electronic Records*	11. Attribution of electronic records 12. Acknowledgment of receipt 13. Time and place of dispatch and receipt of electronic record
CHAPTER V	*Secure Electronic Records and Secure Electronic Signature*	14. Secure electronic record 15. Secure digital signature 16. Security procedures and practices
CHAPTER VI	*Regulation of Certifying Authorities*	17. Appointment of Controller and other officers 18. Functions of Controller 19. Recognition of foreign Certifying Authorities 20. Controller to act as repository 21. License to issue Digital Signature Certificates 22. Application for license 23. Renewal of license 24. Procedure for grant or rejection of license 25. Suspension of license 26. Notice of suspension or revocation of license 27. Power to delegate 28. Power to investigate contraventions 29. ***Access to computers and data*** 30. Certifying Authority to follow certain procedures 31. Certifying Authority to ensure compliance of the Act, etc. 32. Display of license 33. Surrender of license 34. Disclosure

(*Continued*)

Table 6.6 | (*Continued*)

Chapter Number	*Chapter Title*	*Names of the Sections in the Chapter*
CHAPTER VII	*Electronic Signature Certificates*	35. C***ertifying Authority to issue Digital Signature Certificate***
		36. Representations upon issuance of Digital Signature Certificate
		37. Suspension of Digital Signature Certificate
		38. Revocation of Digital Signature Certificate
		39. Notice of suspension or revocation
CHAPTER VIII	*Duties of Subscribers*	40. Generating key pair
		41. Acceptance of Digital Signature Certificate
		42. Control of private key
CHAPTER IX	*Penalties, Compensation and Adjudication*	43. **Penalty for damage to computer, computer system, etc.**
		44. Penalty for failure to furnish information return, etc.
		45. Residuary penalty
		46. Power to adjudicate
		47. Factors to be taken into account by the adjudicating officer
CHAPTER X	*The Cyber Regulations Appellate Tribunal*	48. Establishment of Cyber Appellate Tribunal
		49. Composition of Cyber Appellate Tribunal
		50. Qualifications for appointment
		51. Term of office, conditions of services, etc.
		52. Salary, allowances and other terms and conditions of service of Presiding Officer
		53. Filling up of vacancies
		54. Resignation and removal
		55. Orders constituting Appellate Tribunal
		56. Staff of the Cyber Appellate Tribunal
		57. Appeal to Cyber Appellate Tribunal
		58. Procedure and powers of the Cyber Appellate Tribunal
		59. Right to legal representation
		60. Limitation
		61. Civil Court not to have jurisdiction
		62. Appeal to High Court
		63. Compounding of contraventions
		64. Recovery of penalty or compensation
CHAPTER XI	*Offences*	65. ***Tampering with computer source documents***
	66A. *Punishment for offensive messages*	66. ***Computer-related offences***
	66B. *Punishment for dishonestly receiving stolen computers, etc.*	67. Punishment for publishing, transmitting obscene material in electronic form

(*Continued*)

Table 6.6 | (*Continued*)

Chapter Number	*Chapter Title*	*Names of the Sections in the Chapter*
	66C. *Punishment for ID theft* 66D. *Punishment for cheating by personation with use of computers* 66E. *Punishment for privacy violation* 66F. *Punishment for cyber terrorism*	68. Power of Controller to give directions 69. Power to issue directions for inception or monitoring or decryption of information 70. Protected system 71. ***Penalty for misrepresentation*** 72. ***Penalty for breach of confidentiality and privacy*** 73. ***Penalty for publishing Digital Signature Certificate false in certain particulars*** 74. ***Publication for fraudulent purpose*** 75. Act to apply for offence or contravention committed outside India 76. Confiscation 77. Compensation, penalties or confiscation not to interfere with other punishments 78. Power to investigate offences
CHAPTER XII	*Intermediaries not to be Liable in certain Cases*	79. Exemption from liability of intermediary in certain cases
CHAPTER XIII	*Miscellaneous*	80. Power of police officer and other officers to enter, search, etc. 81. Act to have overriding effect 82. Chairperson, Members, officers and employees to be public servants 83. Power to give directions 84. Protection of action taken in good faith 85. Offences by companies 86. Removal of difficulties 87. Power of Central Government to make rules 88. Constitution of Advisory Committee 89. Power of Controller to make regulations 90. Power of State Government to make rules

Note: Digital signature and cryptography concepts, use of symmetric and asymmetric keys, etc. related concepts are explained in Ref. #7, Books, Further Reading. Readers must refer to the paper copy of the IT Act.

From Table 6.6, we can see that in particular, Sections 65, 66, 67, 71, 72, 73 and 74 in CHAPTER XI (Offences) of the Indian ITA 2000 are relevant to the discussion of cybercrime in legal context. The relevant portion from that is as follows:

1. **Section 65: Tampering with computer source documents**
   Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer

programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to 3 years, or with fine which may extend up to 2 lakh rupees (₹ 2,00,000), or with both.

Explanation: For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

2. **Section 66: Computer-related offences**
   (1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.
   (2) Whoever commits hacking shall be punished with imprisonment up to 3 years, or with fine which may extend up to 5 lakh rupees (₹ 5,00,000), or with both.
3. **Section 67: Punishment for publishing or transmitting obscene material in electronic form**
   Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to 3 years and with fine which may extend to 5 lakh rupees (₹ 5,00,000) and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to 5 years and also with fine which may extend to 10 lakh rupees (₹ 10,00,000).
4. **Section 71: Penalty for misrepresentation**
   Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to 2 years, or with fine which may extend to 1 lakh rupees (₹ 1,00,000), or with both.
5. **Section 72: Penalty for breach of confidentiality and privacy**
   Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made there-under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to 2 years, or with fine which may extend to 1 lakh rupees (₹ 1,00,000), or with both.
6. **Section 73: Penalty for publishing Digital Signature Certificate false in certain particulars**
   (1) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that:
      (a) The Certifying Authority listed in the certificate has not issued it; or
      (b) the subscriber listed in the certificate has not accepted it; or
      (c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.
   (2) Any person who contravenes the provisions of subsection (1) shall be punished with imprisonment for a term which may extend to 2 years, or with fine which may extend to 1 lakh rupees (₹ 1,00,000), or with both.

7. **Section 74: Publication for fraudulent purpose**
   Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to 2 years, or with fine which may extend to 1 lakh rupees (₹ 1,00,000), or with both.

Table 6.7 presents the brief overview of the significant changes brought out by the IT Amendment Bill 2008. Also refer to Section 6.8.1 (Overview of Changes Made to the Indian IT Act) in which changes are explained in great detail.

Box 6.11 Data Protection and the New Clause 43A under the Amended IT Act

The amended Indian IT Act provides for penalty for *damage to computers, computer systems* under the title *Penalty and Adjudication* in *Section 43* that is widely interpreted as a clause to provide data protection in the country. *Unauthorized access to a computer, computer system* or *computer network* is punishable with a compensation of up to 1 crore rupees (₹ 1,00,00,000). This section has been improved to include stealing of computer *source code* for which compensation can be claimed. (Computer source has been defined.) *Data protection* has now been made more explicit through insertion of a *new Clause 43A* that provides for compensation to an aggrieved person whose personal data including *sensitive personal data* may be compromised by a company, during the time it was under processing with the company, for failure to protect such data whether because of negligence in implementing or maintaining reasonable security practices.

Furthermore, *reasonable security practices and procedures* will constitute those practices and procedures that protect such information from unauthorized access, damage, use, modification, disclosure or impairment as may be specified in an agreement between the parties or as may be specified in any law in force. In the absence of such an agreement or any law, the Central Government will prescribe security practices and procedures in consultation with professional bodies or associations:

(a) This explanation gives scope for recognition of security professional bodies such as Data Security Council of India (DSCI), which is an industry initiative promoted by NASSCOM. The best practices and standards for security that DSCI may prescribe to the IT and BPO companies may be accepted by the government. Regulation of companies for compliance with such standards and practices can fall within the ambit of DSCI.

(b) *Sensitive personal information* may be prescribed by the Central Government in consultation with professional bodies or associations. In the context of outsourcing to India, this can be defined to be in line with compliance requirements of the EU (European Union) Data Protection Directive and US laws such as Health Insurance Portability and Accountability Act (HIPAA) or Graham-Leach-Bliley Act (GLBA).

Penalty for breach of confidentiality and privacy: Under Section 72, it is presently restricted to those who gain access to an electronic record or document under the powers conferred under this Act. A new Section 72A has been added that provides punishment for disclosure of information in breach of a lawful contract. Any person including an intermediary who has access to any material containing personal information about another person, as part of a lawful contract, discloses it without the consent of the subject person will constitute a breach and attract punishment with imprisonment of up to 3 years and/or a fine of 5 lakh rupees (₹ 5,00,000). This is a strong deterrent, and also will bring those responsible for breaching data confidentiality, under lawful contracts, to justice. Along with Section 43A, Section 72A strengthens the data protection regime in the country. It will go a long way in promoting trust in transborder data-flows to India.

Note: This information is as per the NASSCOM Whitepaper "Data Protection and Cyber Crime under amended IT Act." The whitepaper was released by DSCI in December 2008. Data Security Council of India (DSCI) is an initiative under NASSCOM.

Table 6.7 | Summary of changes to the Indian IT Act (significant changes brought out by the IT Amendment Bill 2008)

Section No.	*Changes Made*
1	Section 1(4) list of excluded documents removed. To be notified through Gazette.
2	Section 2(d) modified, and the term "Digital Signature" replaced with "Electronic Signature" in the Act. Section 2(ha) added to define "Communication Device" which will include mobile phones, ATM, PDAs, etc. Section 2(j) "Computer Systems" and "Communication Devices" and "Wire" and "Wireless" added. Section 2(k) "Communication Device" added. Section 2(na) introduced to define the term "Cyber Cafe." Section 2(nb) introduced to define the term "Cyber Security." Section 2(ta) and Section 2(tb) introduces the term of "Electronic Signature" and "Electronic Signature Certificate." Section 2(ua) defines "Indian Computer Emergency Response Team." Section 2(v) "Message" included in the definition of "Information." Section 2(w) "Intermediary" defined. It includes telecom. *Note*: **Service providers, network service providers, Internet service providers, webhosting service providers, search engines, online payment sites, online auction** sites, online market places and cyber cafes.
3	Section 3 now refers to legal recognition of electronic documents. New Section 3A introduced to define Electronic Signature.
4 and 5	No significant change.
6	New Section 6A introduced to provide for appointment of service providers in E-Governance services and enable delivery of services by private service providers.
7	New Section 7A introduced to make audit of electronic documents mandatory wherever the legally physical records were subject to audit.
8 and 9	No change.
10	No significant change. New Section 10A specifies that contract formation is possible with offer and acceptance being in electronic form.
11, 12, 13 and 14	No significant change.
15 and 16	Defines "Secured Electronic Signature" and redefines "Security Procedure."
17, 18, 19	No significant change.
20	Section omitted.
21	No significant change.
22 and 23	The amount of specified upper limit on the fees omitted.
24, 25, 26, 27	No significant change.
28 and 29	The powers of Controller have been restricted to contraventions under chapter VI.
30	Consequential Changes with introduction of Electronic Signatures.
31, 32, 33, 34	No significant change.
35	Subsection 35(4) modified.
36	Additional points to be added in the certificate indicated.

(*Continued*)

Table 6.7 | (*Continued*)

Section No.	*Changes Made*
37, 38, 39	No change.
40	No change in Section 40 but a new section added as mentioned below. New Section 40A specifies the duties of the subscriber of Electronic Signatures Certificate.
41 and 42	No change.
43	Two new contraventions added – Contraventions corresponding to earlier Section 65 and Section 66 added for civil liability. Compensation limit removed. New Section 43A included for "Data Protection" need specifies liability for a body corporate handling sensitive data, introduces concept of "reasonable security practices" and sensitive personal data. No limit for compensation.
44 and 45	No significant change.
46	The powers of the Adjudicator limited for claims upto ₹ 5 crore (₹ 5,00,00,000). Civil Court's authority introduced for claims beyond ₹ 5 crore (₹ 5,00,00,000).
47	No significant change.
48	Changes name of Cyber Regulations Appellate Tribunal to Cyber Appellate Tribunal.
49	Cyber Appellate Tribunal (CAT) is made a multimember entity. Provision for benches introduced, non-judicial members can be members of the Tribunal.
50	Specifies qualifications for appointment of Chairperson and Members of the CAT.
51 and 52	Specifies terms and other conditions of appointment of Chairman and Members of CAT (Cyber Appellate Tribunal). New Sections 52A, B, C and D introduced defining powers of the Chairperson of CAT for conduct of business.
53, 54, 55, 56	No significant change.
57, 58, 59, 60	No change.
61	Amended to accommodate jurisdiction of Civil Courts for disputes involving claims of over ₹ 5 crore (₹ 5,00,00,000).
62 and 63	No change.
64	No significant change.
65	No change.
66	*Note:* This is a notable feature of the changes made – note the "punishments." The clause has been rewritten with significant changes. Applies to all contraventions listed in Section 43 and shall be punishable with imprisonment for a term which may extend to three(3) years or with fine which may extent up to ₹ 5 lakhs (₹ 5,00,000) and both. The section applies if act is done "dishonestly" or "fraudulently" as defined in CrPC (Criminal Procedure Code). New Sections added under 66A, 66B, 66C, 66D, 66E and 66F to cover new offences. Section 66A: Sending offensive messages. Punishment: Imprisonment for a term which may extend to three years and fine. Section 66B: Receiving a Stolen Computer Resource Punishment: Imprisonment for a term which may extend to three years or with fine which may extend to rupees one lakh (₹ 1,00,000) or with both.

(*Continued*)

Table 6.7 | (*Continued*)

Section No.	*Changes Made*
	Section 66C: Identity Theft Punishment: Imprisonment for a term which may extend to three years also be liable to fine which may extend to rupees one lakh (₹ 1,00,000). **Section 66D: Cheating by personation** Punishment: Imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees (₹ 1,00,000). **Section 66E: Violation of Privacy** Punishment: Imprisonment for a term which may extend to three years or with fine not exceeding two lakh rupees (₹ 2,00,000) or with both. **Section 66F: Cyber Terrorism** Punishment: Imprisonment which may extend to imprisonment for life.
67	Fine increased to ₹ 5 lakhs (₹ 5,00,000) for first instance and ₹ 10 lakhs (₹ 10,00,000) for subsequent instance. Imprisonment reduced to three years for first instance and 5 years for subsequent instance. New Section 67A introduced to cover material containing "sexually explicit act." Punishment: On first conviction with imprisonment for a term which may extend to five years and with fine which may extent to 10 lakhs (₹ 10,00,000). In the event of second and subsequent conviction with imprisonment for a term which may extend to seven years and also with fine which may extent to 10 lakhs (₹ 10,00,000). New Section 67B introduced to cover child explicit act or conduct. Punishment: On first conviction with imprisonment for a term which may extend to five years and with fine which may extent to 10 lakhs (₹ 10,00,000). In the event of second and subsequent conviction with imprisonment for a term which may extend to seven years and also with fine which may extent to 10 lakhs (₹ 10,00,000). New Section 67C: This provision will require Intermediaries to preserve and retain certain records for a stated period. Punishment: Imprisonment for a term which may extend to three years and also be liable to pay fine.
68	Refers to the powers of the Controller to direct Certifying Authorities for compliance. No significant change. Penal powers to be applicable only on intentional violation.
69	Scope extended from decryption to interception, monitoring also. Power lies with the authorized government agency of the Central Government. New Section 69A: Introduced to enable blocking of websites. If an Intermediary is not cooperative. Punishment: Imprisonment for a term which may extent to seven years and also be liable to fine. New section 69B: Provides powers for monitoring and collecting traffic data, etc. If an Intermediary is not cooperative. Punishment: Imprisonment for a term which may extent to three years and also be liable to fine.
70	Critical Infrastructure System defined and section restricted to only such systems. Security practices to be notified.
70B	New Section 70A: Added to define National Nodal Agency for Critical Information Infrastructure Protection. Indian Computer Emergency Response Team (Cert India) appointed as the Nodal agency for incident response.
71 and 72	No change. New Section 72A: Introduced for punishment for **disclosure of information in breach of lawful Contract** (data protection purpose).

(*Continued*)

Table 6.7 | (*Continued*)

Section No.	*Changes Made*
73, 74, 75, 76	No change.
77	No significant change. New Section 77A: Introduced to provide for Compounding of offences other than offences for which imprisonment for life or imprisonment for a term exceeding three years has been provided. New Section 77B: Introduced to consider all offences punishable with imprisonment of three years and above under the Act as Cognizable offence and offence punishable with imprisonment for 3 years as bailable.
78	Power to investigate any cognizable offence vested with Inspectors instead of DSPs (Deputy Superintendent of Police). *Note:* This is notable change of bringing down the investigation authority lower in the hierarchy.
79	Exemption from liability of intermediary in certain cases – some exceptions have been added – no liability if intermediary provides only Internet access, observed due diligence, had no actual knowledge of offence, etc. New Section 79 A: Introduced to provide for the government to designate any government body as an Examiner of Electronic Evidence.
80	The powers, earlier available to DSPs, is now made available to Inspectors. *Note*: This is notable change of bringing down the investigation authority lower in the hierarchy.
81	Amended to keep the Copyright and Patent Acts fully applicable.
81A	No change.
82	No significant change.
83 and 84	No change. Section 84A: New section introduced to enable the government to prescribe encryption methods. New Section 84B: Introduced to make "abetment" punishable as the offence itself is under the IT Act 2000. New Section 84C: Introduced to make an "attempt to commit an offence" punishable with half of the punishment meant for the offence.
85 and 86	No change.
87	Consequential changes made.
88 and 89	No change.
90	No significant change.
91–94	Omitted

Box 6.12 Digital Evidence and its Admissibility in Courts

Digital/electronic evidence is probative information stored in digital form that a party may use at trial. It includes computer printouts, E-Mails, digital photographs, ATM transaction logs, spreadsheets and others. With increased computerization and technology as well as the rise of the digital office, courts have been forced to allow for the admittance of digital evidence. In the Indian ITA 2000, the word *Evidence* appears in Section 58 (Procedure and Powers of the Cyber Appellate Tribunal), The Second Schedule, Clause 65B (Admissibility of Electronic Records). It is said that the enactment and adoption of the Indian Evidence Act was a path-breaking judicial measure introduced in India, which changed the entire system of concepts pertaining to admissibility of evidences in the Indian Courts of Law.

Box 6.12 Digital Evidence and . . . (*Continued*)

There are challenges in digital evidence handling. Today, the computer technology is very complex, although the usability for the end-users is very high. The extensive amount of data stored on today's computers and the limited resources available to analyze computer evidence are two of the facts that contribute to delays in the return of digital evidence. With the worldwide reach of the Internet, crimes are no longer easily defined as occurring within a particular city, state or even within the country. More and more criminals are coming from around the world and committing crimes against their targeted victims via the Internet. In such situations, law enforcement officials may find it difficult to obtain evidence and even impossible to enforce warrants for searches and seizures of digital evidence stored abroad. The complexity of most types of digital evidence, as well as the methods in which law enforcement comes into control of the evidence, can raise issues of admissibility, that is, admissibility of digital evidence. Courts have noted very important differences. As compared to the more traditional evidence, courts have noted that digital evidence tends to be more voluminous, more difficult to destroy, easily modified, easily duplicated, potentially more expressive and more readily available. More about digital evidence is addressed in Chapters 7 and 8.

6.4.1 Admissibility of Electronic Records: Amendments made in the Indian ITA 2000

The Second, the Third and the Fourth Schedule of the Indian ITA 2000 indicates how the three acts, namely, The Indian Evidence Act 1872, The Bankers' Books Evidence Act 1891 and The Reserve Bank of India Act 1934 have been amended. In this section, these amendments are presented. This is particularly important for the discussion about forensics in Chapter 7. It appears that the maximum amendments have been made to the Indian Evidence Act.

In the Indian Evidence Act, CHAPTER IV is about Oral Evidence and CHAPTER V is about Documentary Evidence. In the Indian IT Act, the Second Schedule presents "Amendments to the Indian Evidence Act of 1872." The text from there pertaining to the amendment is presented below.

The Second Schedule of the Indian ITA 2000: Amendment to the Indian Evidence Act

1. In Section 3:
   (a) In the definition of "Evidence," for the words "all documents produced for the inspection of the Court," the words "all documents including electronic records produced for the inspection of the Court" shall be substituted;
   (b) after the definition of "India," the following shall be inserted, namely, the expressions "Certifying Authority," "digital signature," "Digital Signature Certificate," "electronic form," "electronic records," "information," "secure electronic record," "secure digital signature" and "subscriber" shall have the meanings, respectively, assigned to them in the Information Technology Act 2000.

2. In Section 17, for the words "oral or documentary," the words "oral or documentary or contained in electronic form" shall be substituted.

3. After Section 22, the following section shall be inserted, namely, when oral admission as to contents of electronic records is relevant.

"22A. Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question."

4. In Section 34, for the words "Entries in the books of account," the words "Entries in the books of account, including those maintained in an electronic form" shall be substituted.

5. In Section 35, for the word "record," in both the places where it occurs, the words "record or an electronic record" shall be substituted.

6. For Section 39, the following section shall be substituted, namely, *What evidence to be given when statement forms part of a conversation, document, electronic record, book or series of letters or papers.*

"39. When any statement of which evidence is given forms part of a longer statement, or of a conversation or pan of an isolated document, or is contained in a document which forms part of a book, or is contained in part of electronic record or of a connected series of letters or papers, evidence shall be given of so much and no more of the statement, conversation, document, electronic record, book or series of letters or papers as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made."

7. After Section 47, the following section shall be inserted, namely, *Opinion as to digital signature where relevant.*

"47A. When the Court has to form, an opinion as to the digital signature of any person, the opinion of the Certifying Authority which has issued the Digital Signature Certificate is a relevant fact."

8. In Section 59, for the words "contents of documents" the words "contents of documents or electronic records" shall be substituted.

9. After Section 65, the following sections shall be inserted, namely, *Special provisions as to evidence relating to electronic record.*

"65A. The contents of electronic records may be proved in accordance with the provisions of Section 65B."

Admissibility of Electronic Records

65B. (1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

(2) The conditions referred to in subsection (1) in respect of a computer output shall be the following, namely,

(a) The computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents and

(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

(3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in Clause (a) of subsection (2) was regularly performed by computers, whether:
(a) By a combination of computers operating over that period; or
(b) by different computers operating in succession over that period; or
(c) by different combinations of computers operating in succession over that period; or
(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers, all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say:
(a) Identifying the electronic record containing the statement and describing the manner in which it was produced;
(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;
(c) dealing with any of the matters to which the conditions mentioned in subsection (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this subsection it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section:
(a) Information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;
(b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;
(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Explanation: For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived there-from by calculation, comparison or any other process.

10. After Section 67, the following section shall be inserted, namely, *Proof as to digital signature.*

"67A. Except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record the fact that such digital signature is the digital signature of the subscriber must be proved."

11. After Section 73, the following section shall be inserted, namely, *proof as to verification of digital signature.*

"73A. In order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the Court may direct:

(a) That person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;

(b) any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person."

Explanation: For the purposes of this section, "Controller" means the Controller appointed under subsection (1) of Section 17 of the Information Technology Act 2000.

12. Presumption as to Gazettes in electronic forms

After Section 81, the following section shall be inserted, namely,

"81A. The Court shall presume the genuineness of every electronic record purporting to be the Official Gazette, or purporting to be electronic record directed by any law to be kept by any person, if such electronic record is kept substantially in the form required by law and is produced from proper custody."

13. Presumption as to electronic agreements

After Section 85, the following sections shall be inserted, namely,

"85A. The Court shall presume that every electronic record purporting to be an agreement containing the digital signatures of the parties was so concluded by affixing the digital signature of the parties."

14. Presumption as to electronic records and digital signatures

85B (1) In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved that the secure electronic record has not been altered since the specific point of time to which the secure status relates.

(2) In any proceedings, involving secure digital signature, the Court shall presume unless the contrary is proved that:

(a) The secure digital signature is affixed by subscriber with the intention of signing or approving the electronic record;

(b) except in the case of a secure electronic record or a secure digital signature, nothing in this section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature.

15. Presumption as to Digital Signature Certificates

85C The Court shall presume, unless contrary is proved, that the information listed in a Digital Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber.

16. Presumption as to electronic messages

After Section 88, the following section shall be inserted, namely,

"88A. The Court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent."

Explanation: For the purposes of this section, the expressions "addressee" and "originator" shall have the same meanings, respectively, assigned to them in Clauses (b) and of subsection (1) of Section 2 of the Information Technology Act 2000.

17. Presumption as to electronic records of five years old

After Section 90, the following section shall be inserted, namely,

"90A. Where any electronic record, purporting or proved to be five years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that

the digital signature which purports to be the digital signature of any particular person was so affixed by him or any person authorized by him in this behalf."

Explanation: Electronic records are said to be in proper custody if they are in the place in which, and under the care of the person with whom, they naturally be; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render such an origin probable. This explanation applies also to Section 81A.

For Section 131, the following section shall be substituted, namely, production of documents or electronic records which another person, having possession, could refuse to produce.

131. No one shall be compelled to produce documents in his possession or electronic records under his control, which any other person would be entitled to refuse to produce if they were in his possession or control, unless such last-mentioned person consents to their production.

The Third Schedule of the Indian IT Act 2000: Amendment to the Bankers' Books Evidence Act

1. In Section 2:

(a) For Clause (3), the following clause shall be substituted, namely, '(3) "bankers' books" include ledgers, day-books, cash-books, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device;

(b) for Clause (8), the following clause shall be substituted, namely, '(8) "certified copy" means when the books of a bank:

(A) Are maintained in written form, a copy of any entry in such books together with a certificate written; the foot of such copy that it is a true copy of such entry, that such entry is contained in one of the ordinary books of the bank and was made in the usual and ordinary course of business and that such book is still in the custody of the bank, and where the copy was obtained by a mechanical or other process which in itself ensured the accuracy of the copy, a further certificate to that effect, but where the book from which such copy was prepared has been destroyed in the usual course of the bank's business after the date on which the copy had been so prepared, a further certificate to that effect, each such certificate being dated and subscribed by the principal accountant or manager of the bank with his name and official title; and

(B) consist of printouts of data stored in a floppy, disc, tape or any other electro-magnetic data storage device, a printout of such entry or a copy of such printout together with such statements certified in accordance with the provisions of Section 2A.

2. After Section 2, the following section shall be inserted, namely, *Conditions in the printout.*

"2A. A printout of entry or a copy of printout referred to in subsection (8) of Section 2 shall be accompanied by the following, namely,

(a) A certificate to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager and

(b) a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of:

(A) The safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorized persons;

(B) the safeguards adopted to prevent and detect unauthorized change of data;

(C) the safeguards available to retrieve data that is lost due to systemic failure or any other reasons;

(D) the manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electro-magnetic data storage devices;
(E) the mode of verification in order to ensure that data has been accurately transferred to such removable media;
(F) the mode of identification of such data storage devices;
(G) the arrangements for the storage and custody of such storage devices;
(H) the safeguards to prevent and detect any tampering with the system and
(I) any other factor which will vouch for the integrity and accuracy of the system.

(c) a further certificate from the person in-charge of the computer system to the effect that to the best of his knowledge and belief, such computer system operated properly at the material time, he was provided with all the relevant data and the printout in question represents correctly, or is appropriately derived from, the relevant data."

The Fourth Schedule of the Indian IT Act 2000: Amendment to the Reserve Bank of India Act

In the Reserve Bank of India Act 1934, in Section 58, in subsection (2), after Clause (p), the following clause shall be inserted, namely,

"the regulation of fund transfer through electronic means between the banks or between the banks and other financial institutions referred to in Clause (c) of Section 45-1, including the laying down of the conditions subject to which banks and other financial institutions shall participate in such fund transfers, the manner of such fund transfers and the rights and obligations of the participants in such fund transfers."

6.4.2 Positive Aspects of the ITA 2000

The Indian ITA 2000, though heavily criticized for not being specific on cybercrimes, in our opinion, does have a few good points. At the same time, there is, also, fair amount of vagueness in the Act. This is briefly discussed here in this section.

1. Prior to the enactment of the ITA 2000 even an E-Mail was not accepted under the prevailing statutes of India as an accepted legal form of communication and as evidence in a court of law. But the ITA 2000 changed this scenario by legal recognition of the electronic format. Indeed, the ITA 2000 is a step forward.
2. From the perspective of the corporate sector, companies are able to carry out E-Commerce using the legal infrastructure provided by the ITA 2000. Till the coming into effect of the Indian cyberlaw, the growth of E-Commerce was impeded in our country basically because there was no legal infrastructure to regulate commercial transactions online.
3. Corporate will now be able to use digital signatures to carry out their transactions online. These digital signatures have been given legal validity and sanction under the ITA 2000.
4. In today's scenario, information is stored by the companies on their respective computer system, apart from maintaining a backup. Under the ITA 2000, it became possible for corporate to have a statutory remedy if anyone breaks into their computer systems or networks and causes damages or copies data. The remedy provided by the ITA 2000 is in the form of monetary damages, by the way of compensation, not exceeding ₹ 10,000,000.
5. ITA 2000 defined various cybercrimes. Prior to the coming into effect of the Indian Cyberlaw, the corporate were helpless as there was no legal redress for such issues. However, with the ITA 2000 instituted, the scenario changed altogether.

6.4.3 Weak Areas of the ITA 2000

As mentioned before, there are limitations too in the IT Act; those are mainly due to the following gray areas:

1. The ITA 2000 is likely to cause a conflict of jurisdiction.
2. E-Commerce is based on the system of domain names. The ITA 2000 does not even touch the issues relating to domain names. Domain names have not been defined and the rights and liabilities of domain name owners do not find any mention in the law. The law does not address the rights and liabilities of domain name holders.
3. The ITA 2000 does not deal with issues concerning the protection of Intellectual Property Rights (IPR) in the context of the online environment. Contentious yet very important issues concerning online copyrights, trademarks and patents have been left untouched by the law, thereby leaving many loopholes. Thus, the law lacks "Proper Intellectual Property Protection for Electronic Information and Data" – the law misses out the issue of IPR, and makes no provisions whatsoever for copyrighting, trade marking or patenting of electronic information and data. However, the corresponding provisions are available under the Indian Copyright Act (refer to Appendix T in CD).
4. As the cyberlaw is evolving, so are the new forms and manifestations of cybercrimes. The offenses defined in the ITA 2000 are by no means exhaustive. However, the drafting of the relevant provisions of the ITA 2000 makes it appear as if the offenses detailed therein are the only cyberoffenses possible and existing. The ITA 2000 does not cover various kinds of cybercrimes and Internet-related crimes. These include:
   - Theft of Internet hours (see for more details in Chapter 1);
   - cybertheft;
   - cyberstalking (for more details refer to Section 2.4 of Chapter 2);
   - cyberharassment;
   - cyberdefamation (for more details refer to Section 1.5.3 of Chapter 1);
   - cyberfraud (for more details see Chapter 1);
   - misuse of credit card numbers;
   - chat room abuse;
   - cybersquatting (not addressed directly).
5. The ITA 2000 has not tackled vital issues pertaining to E-Commerce sphere like privacy and content regulation to name a few.
6. The Information Technology Act is not explicit about regulation of Electronic Payments, and avoids applicability of IT Act to Negotiable Instruments. The Information Technology Act stays silent over the regulation of electronic payments gateway and rather segregates the negotiable instruments from the applicability of the IT Act. This may have major effect on the growth of E-Commerce in India. This has led to tendencies of banking and financial sectors being irresolute in their stands.
7. IT Act does not touch upon antitrust issues.
8. The most serious concern about the Indian Cyberlaw relates to its implementation. The ITA 2000 does not lay down parameters for its implementation. Also, when Internet penetration in India is extremely low and government and police officials, in general, are not very computer savvy, the new Indian cyberlaw raises more questions than it answers. It seems that the Parliament would be required to amend the ITA 2000 to remove the gray areas mentioned above.