5.0 Introduction

Human beings were given capable and inquisitive minds, so they seek endlessly better ways of doing things. This drive, coupled with innate curiosity and a strong drive to unlock the secret of nature, has unravelled the secrets of the nature, has created a steady stream of inventions over the years. A principal thrust of innovation today continues towards technological advances that enhance the productivity of labour and free humans to tasks done more economically by machines. Among societies’ newest demand is for the means to handle the vast amount of information generated by modern life. This information explosion stems from the sophisticated business practices, new residential resources, substantially increased record keeping through extensive data bases, and globalization of our advanced society.

The information technology has evolved over many years to assist a growing portion of the work force devoted to the generation, transmission, storage, processing, retrieval, and general use of information. The computer, along with telecommunications, is making today’s information work force more efficient, much as the machines raised production during the industrial revolution. In both cases, societies’ thirst for technology to reduce labour was met in striking ways by a wide range by innovations of various impacts.¹

5.1 Evolution of Information Technology

Since World War II, the performance capabilities of computers and telecommunications have been doubling every few years at constant cost. For example, a decade ago $3,500 could buy a new Apple II microcomputer. Today, $6,800 — the same amount of purchasing power (adjusted for 10 years of inflation) — can buy a new

¹ https://project2061.org/publications/designs/online/pdfs/reprints/8_dede.pdf visited on 19th Jan 2013 at 1.40 pm
Macintosh II microcomputer. The Macintosh handles 4 times the information at 16 times the speed, pre-programmed and reprogrammable memory are both about 20 times larger, disk storage is about 90 times larger, and the display has 7 times the resolution and 16 times the number of colours. Comparable figures could be cited for other brands of machines. Equally impressive, users' demands for this power have increased as rapidly as it has become available.

Over the next two decades, data processing and information systems will probably be replaced by sophisticated devices for knowledge creation, capture, transfer, and use. A similar evolution can be forecast for telecommunications: personal video recorders, optical fibre networks, intelligent telephones, information utilities such as videotext, and digital discs will change the nature of media.

A network is simply a set of interconnected nodes. It may have a hierarchy, but it has no centre. Relationships between nodes are asymmetrical, but they are all necessary for the functioning of the network for the circulation of money, information, technology, images, goods, services, or people throughout the network. The most critical distinction in this organizational logic is not stability, but inclusion or exclusion. Networks change relentlessly: they move along, form and re-form, in endless variation. Those who remain inside have the opportunity to share and, over time, to increase their chances. Those who drop out, or become switched off, will see their chances vanish.²

It is urgently necessary to reverse the downward spiral of exclusion and to use information and communication technologies to empower humankind. The reintegration of social development and economic growth in the information age will require massive technological upgrading of countries, firms and households around the world- a strategy of the highest interest for everyone, including business. It will take a dramatic investment in overhauling the educational system everywhere. It will require the establishment of a worldwide network of science and technology, in which the most advanced universities, will be willing to share knowledge and expertise for the common good. It must aim at reversing, slowly but surely, the marginalization of entire countries, or cities or

² Ibid
neighbourhoods, so that the human potential that is currently being wasted can be reinvested.  

5.1.1 Nature and Concept of Information Technology

Information technology is not the cause of the changes we are living through. But without new information and communication technologies none of what is changing our lives would be possible. In the 1990s the entire planet is organized around telecommunicated networks of computers at the heart of information systems and communication processes. The entire realm of human activity depends on the power of information, in a sequence of technological innovation that accelerates its pace by month. Genetic engineering, benefiting from this wealth of information processing capacity, is progressing by leaps and bounds, and is enabling us, for the first time, to unveil the secrets of living matter and to manipulate life, with extraordinary potential consequences. Software development is making possible user-friendly computing, so that millions of children, when provided with adequate education, can progress in their knowledge, and in their ability to create wealth and enjoy it wisely, much faster than any previous generation. Internet- today used by about 100 million people, and doubling this number every year- is a channel of universal communication where interests and values of all sorts coexist, in a creative cacophony. Certainly, the diffusion of information and communication technology is extremely uneven. Most of Africa is being left in a technological apartheid, and the same could be said of many other regions of the world. The situation is difficult to remedy when one third of the worlds' population still has to survive on the equivalent of one dollar per day.

The crucial role of information and communication technologies in stimulating development is a two-edged sword. On the one hand, it allows countries to leapfrog stages of economic growth by being able to modernize their production systems and increase their competitiveness faster than in the past. The most critical example is that of

\(^1\)Ibid
\(^4\)http://www.itcon.org/2002/8/paper.pdf visited 16\(^{th}\) January 2013 at 1.58 pm
\(^5\)http://www.csi-india.org/c/document_library/get_file?uuid=398e08b8-436f-4ff6-a2190a3b2c7c3861&groupId=10616 visited on 16th Jan 2013 at 1.58 pm
the Asian Pacific economies, and particularly the cases of Hong Kong, Taiwan, Singapore, Malaysia and South Korea. This is so despite the current financial crisis, which is unrelated to competitive performance and may be related, in fact, to the attractiveness of booming Asian economies to global capital flows. On the other hand, for those economies that are unable to adapt to the new technological system, their retardation becomes cumulative. Furthermore, the ability to move into the Information Age depends on the capacity of the whole society to be educated, and to be able to assimilate and process complex information. This starts with the education system, from the bottom up, from the primary school to the university. And it relates, as well, to the overall process of cultural development, including the level of functional literacy, the content of the media, and the diffusion of information within the population as a whole.

5.1.2 Impulsiveness of Information Technology

Many Information Technology applications conceived from the perspective of a rationalistic explanation of how Information Systems are used in an organization exhibit Tayloristic work design, focusing on the individual’s task productivity while underestimating the importance of the social context. This often leads to inappropriate application designs, difficulty of use and outright failure of many Information Technology systems. But what is often forgotten, according to Chaharbaghi and Willis, is that the relationship between humankind and technology has existed since human first walked the earth, the term technology itself originates from the Greek word, “techne”, meaning the art of making perfect what seems imperfect in nature and “logy” meaning the study of. Technology is not about things – tools, processes, and products; it is about work – the specifically human activity by means of which man pushes back the limitations of the iron biological law. Technology forms some sort of a paradox where individual’s survival depends on it, but their problems derive from it. Information Technology has a number of distinctive features that make its potential to influence social change (social factors) very significant, these features include:

1) **Ubiquitous application** – Individuals irrespective of the type of business or role they perform can apply Information Technology in many different ways. E.g. an e-mail system, Internet access or data processing capability is just as relevant to a hospital as
to a component manufacturer. In fact it is highly likely that they will use similar hardware and software and could communicate and exchange data quickly and easily should they need to.6

2) Dramatic rate of cost decline – The price of processing power, data storage and transmission has decreased dramatically. E.g. a “Furby” toy contains more processing power than was once used on the Apollo space programme.

3) Universal ownership – The increasing utility and ever lower cost of hardware and software means that they are now almost universally adopted. However the availability of bandwidth to enable rapid communication and transmission of data remains problematic in many countries and is therefore, a block to further development.7

4) Exponential growth – Rapid development and innovation will lead to cost reduction and an increase in capacity. E.g. with surplus capacity in recently installed fibre optic network apparent, due to recent further technology gains, this in turn is likely to stimulate more development.

The European Union and the United States, the world’s leaders in the fields of innovation and high technology, share a common set of values based on a commitment to democracy, human rights, market economics, and the rule of law. But EU and US approaches to many technology related issues in law and policy differ significantly, causing barriers to trade across the Atlantic and legal uncertainty within the Transatlantic Marketplace, which comprises about 450 million people in the EU and 300 million people in the US.

5.2 Information Technology Law in the USA

The introduction of computers and the Internet in private and government offices opened the doors to a complex and new world of business. This new world was full of windows of opportunities for the ill-intentioned and severely devoid of strong doors with locks. Several laws have been passed to secure those doors of ill-intent while maintaining windows for the public. One such law is the Federal Information Security and

6 http://www3.weforum.org/docs/Global_IT_Report_2012.pdf visited 16th January 2013 at 2.10 pm
7 Ibid at 6
Management Act (FISMA). Enacted in December 2002 as part of the E-Government Act of 2002, government entities and subsequently their contractors have been hurried to comply with the law. Since its inception there have been several guidelines established to help government entities conform with FISMA.\(^8\)

5.2.1 Brief History

The Federal Information Security Management Act (FISMA)\(^9\) when signed into law by the President as part of the E-Government Act of 2002 permanently reauthorized and amended several previous laws. Whether it was a goal of reducing or eliminating paper waste in the government, standardizing technologies and processes, or securing our government resources, all of these laws were designed to give the federal government an upper edge in addressing the changing world of technology.

The first laws (Government Paper Reduction Act of 1980 and 1995\(^10\) (PRA) and Government Paper Elimination Act of 1998\(^11\) (GPEA) were meant to move the federal government from a paper-based bureaucracy, where inconsistencies across agencies led to wasted money and resources, to a “efficient, effective and economical”\(^12\) government that shared information and resources taking advantage of technology and all it had to offer. Soon to follow were laws (Computer Security Act of 1987\(^13\) (CSA) and The Information Technology Management Reform Act of 1996\(^14\) (Clinger-Cohen Act)) designed to secure the federal IT infrastructure as well as emphasize “a risk-based policy for cost effective security.”\(^15\) In order to assist federal agencies comply with these laws,
the Office of Management and Budget (OMB) released Circular A-130, Appendix A Security of Federal Automated Information Resources. Circular A-130 required federal agencies to:

i) "Plan for security;
ii) Ensure that appropriate officials are assigned security responsibility;
iii) Periodically review the security controls in their information systems; and
iv) Authorize system processing prior to operations and, periodically, thereafter."\(^{16}\)

The Government Information Security Reform Act (GISRA)\(^{17}\), signed into law as part of the National Defence Authorization Act of 2000, addressed the issues of program management and required further assessment and reporting of information security. This law was not permanent, however, and was scheduled to sunset in November 2001. FISMA was introduced, as part of the E-Government Act, making the provisions under GISRA permanent. The goal of FISMA, in short, is to "require each federal agency to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source."\(^{18}\)

5.2.2 Laws Applicable to Federal Contractors

Perhaps one of the most difficult aspects of IT security and C&A understands which federal laws must be complied with and by whom and this is without considering local and state legislation. It could be assumed that CIOs, Security Officers and others under their direction at the federal agencies would know which laws apply and how they apply to their programs and subsequently their contractors. That is not always the case, however. The fact is there are so many Acts, presidential Executive Orders and official guidelines that it really is not so simple. Perhaps the best reference are the Acts and

\(^{16}\) *Ibid*


Executive Orders themselves because most have sections dedicated to listing the applicable and associated laws that are either superseded or act as references. That assumes though, that one already knows which laws apply and know where to find the original text and not just a summary.

The situation for federal contractors becomes a little more confusing. There are much security and IT laws in existence that appear to only address federal agencies. When the laws are read in detail, however, there is often the phrase, to use FISMA as an example: “including those provided or managed by another agency, a contractor or other source”\(^\text{19}\) or something similar imbedded. This phrase requires federal government contractors to adhere to the same mandates as the agency for which they are working. Again, this is not a simple matter and will be discussed further in the “Lessons Learned and Contractor Responsibilities” section of this document.

In trying to determine which laws are applicable, the obvious first choice is to ask the manager, director or security officer at the agency; they should know. New information and directives are not always passed down the chain in a timely manner, so if one wants to be prepared another good place to check is the media. There are many websites dedicated to IT information and many of these sites have sections that focus on federal regulations. These websites have become more prevalent with the recent and very quick enactment of so many laws pertaining to security since the terrorist attacks on 9/11/01. The following non-government websites, while occasionally bias, have proven to be good sources of security legislation information:

GovExec.com (http://www.govexec.com)

The ‘E-Government’ link on the home page leads to a wealth of news, special reports, and links to other related web sites. There is also a “Bill Tracker” link on the home page that leads to a list of current bills going through Congress. It includes a search mechanism for bills and legislation as well as a search by ZIP Code for elected officials. In their own words, “GovExec.com is government’s

\(^{19}\) Federal Information Security Management Act (FISMA) – 3544(b)
business news daily and the premier web site for federal managers and executives.\textsuperscript{20}

Government Computer News (GCN) (http://www.gcn.com)

While the home page lists current news articles on government security issues, following the 'E-Government' link will provide the most concise list.

Washington Technology (http://washingtontechway.com)

Washington Technology provides links to "Budget/Policy/Legislation", "Security", "E-Government" and several other IT security topics containing current news releases and information.

Centre for Democracy and Technology (http://cdt.org)

This site is a watch dog/activist site, so they are slightly biased, but they are very up-to-date on the latest IT legislation and news. "The Centre for Democracy and Technology works to promote democratic values and constitutional liberties in the digital age. With expertise in law, technology, and policy, CDT seeks practical solutions to enhance free expression and privacy in global communications technologies."\textsuperscript{21}

There are a plethora of other websites and news magazines spanning the political spectrum. Anybody should be able to find one that fits their information needs.

5.2.2.1 The Players

Once the applicable federal mandates have been identified, it is important to understand which agencies and entities are responsible for which pieces of the legislation. Knowing which agencies, and subsequently the audience, are involved in the process allows one to focus the process and documentation towards the agency making the

\textsuperscript{20} GovExec.com – About Us - http://govexec.com/about.html visited 16\textsuperscript{th} January 201
\textsuperscript{21} Centre for Democracy and Technology – Mission – http://www.cdt.org/mission visited 16\textsuperscript{th} January 2013
request. It also helps in the general sense of knowing where the document and responsibilities for review and follow-ups will end up.

The Whitehouse (www.whitehouse.gov)

The President is responsible of overseeing the Executive Office of the President, which includes: the Office of Management and Budget (OMB), the National Security Council, the Office of Homeland Security, the Office of Science and Technology Policy, as well as a number of other non-security and information technology related offices. These offices are primarily responsible for advising the President on issues pertaining to their areas of expertise and therefore have significant influence in policy decisions and drafting of Executive Orders.

Office of Management and Budget (OMB) (www.whitehouse.gov/omb)

OMB is required under the Paperwork Reduction Act to “develop and implement uniform and consistent information resources management policies” as well as oversees, evaluate, and measure compliance. OMB is responsible of overseeing C&A and reporting the results to Congress. OMB is included in the Executive Office of the President.

Commerce Department (www.commerce.gov)

The Commerce Department oversees a wide array of topics ranging from trade, economics, statistics, census, weather, and technological innovation. The National Institute of Standards and Technology (NIST) is an agency of the Technology Administration of the Commerce Department.

National Institute of Standards and Technology (NIST) (www.nist.gov)

NIST is an agency of the Technology Administration of the Commerce Department. NIST is responsible for working with industry to “develop and apply

---

23 OMB Circular A-130, Section 5: Background
24 Federal Information Security Management Act (FISMA) – 3543(a)(8)
technology, measurements, and standards.26 The Computer Security Division of the NIST Information Technology Laboratory is responsible for developing information technology standards and guidance on applying these standards. NIST is charged with developing the standards and guidelines for compliance with FISMA27 and OMB Circular A-13028. The 800 series29 documents are especially important in understanding IT security guidelines and mandates including the mandates under FISMA.

Legal and historical traditions have evolved quite differently in the United States than in Europe, and the United States takes a different approach to privacy issues from the EU's. The U.S. legal tradition, rooted in concerns about governmental excesses, has led to a preference for decentralized authority, a reluctance to regulate the private sector absent demonstrated need, and generally greater concern about government excess than about private sector excess. And, while the U.S. Constitution establishes certain privacy protections for individuals, such as the right to be free from warrantless searches, it does not explicitly protect information privacy, nor has any such right been inferred from the Constitution. In addition, a fundamental tenet of American democracy, the First Amendment to the U.S. Constitution, requires a balance between the privacy rights of individuals and the benefits that stem from the free flow of information within and across U.S. borders.

Accordingly, when the U.S. adopted a comprehensive privacy law—the Privacy Act of 1974—it governed only the Federal Government's use of citizens' personal information. Other federal privacy protection statutes apply to specific government agencies or information, such as income tax and census data. Neither federal nor state governments, however, have adopted comprehensive information privacy protections affecting private sector data use. (Some state constitutions, such as those of California, Florida, and Hawaii, explicitly set forth a right to information privacy without specifying any rights relating directly to information privacy.)

26U.S. Commerce Department - NIST - http://www.commerce.gov/organization.html visited 16th January 2013
27 Federal Information Security Management Act (FISMA) – Section 303(a-d)
28 OMB Circular A-130, Section 9c: Assignment of Responsibilities – Department of Commerce
In contrast, the information privacy laws that govern the private sector in the United States were adopted either because of specific instances of abuse, perceived market failure, or because particularly sensitive information and/or groups were involved. There is also concern that information privacy issues differ so across different industry sectors that "a one size fits all" legislative approach would lack the necessary precision to avoid interfering with the benefits that flow from the free flow of information. For that reason, too, the U.S. has adopted limited sector-specific privacy legislation. As a result, a number of statutes cover the collection and use of personal information in specific contexts, such as children’s personal information, information collected by telephone and cable companies and credit bureaus, and financial, video rental and drivers’ license information. A brief review of three of these statutes makes clear that privacy statutes in the U.S. take different approaches and impose different schemes for protecting privacy depending on the circumstances.\(^\text{30}\)

### 5.2.2.2 Fair Credit Reporting Act

Congress enacted the Fair Credit Reporting Act (FCRA) in 1970 to deal with widespread concerns about incorrect and widely disseminated consumer credit reports. The FCRA governs disclosure of consumer credit information by credit bureaus. It starts with the premise that widespread availability of correct credit information to parties with a real need for the information will benefit the U.S. economy. For this reason, it provides consumers with a limited right to consent to the use of their personal information.

The Act imposes strict regulations on who may use the credit information and on ensuring that the information is accurate. It thus limits the disclosure of credit information to businesses with a legitimate need for the information and provides certain rights to consumers when credit information is used to deny them an important benefit. To help ensure accuracy, the Act requires that consumers have access to information maintained about them and sets out fairly prescriptive rules governing how access must be provided. The Act also requires that the recipients of credit reports be identified, prohibits the reporting of obsolete information, and provides a correction process for

\(^{30}\)Supra note 21.
inaccurate or incomplete information. And, if a consumer is denied credit for personal, family, or household purposes or is denied employment and the denial is based on information in a consumer report, the entity receiving the report is required to notify the consumer and identify the credit bureau that furnished the report in question. The FCRA allocates enforcement responsibilities among a number of federal agencies, primarily to the Federal Trade Commission.\textsuperscript{31}

5.2.2.3 Children's Online Protection Act

In October 1998, Congress passed the Children's Online Privacy Protection Act (COPPA). The law applies to operators of commercial web sites and online services that collect or maintain information from web site or service visitors and users and prohibits the collection of information from children under the age of 13 without verifiable parental consent. It also provides for a safe harbor from privacy liability where companies adhere to a self-regulatory program approved by the Federal Trade Commission. The Federal Trade Commission, which was charged with enforcing developing regulations under the statute, issued implementing rules in April 2000.

These rules set out criteria for web site operators and on-line services that are targeted to children or have actual knowledge that the person from whom they seek information is a child. They require notice of what personally identifiable information is being collected, how it will be used, and whether it will be disclosed. Subject to certain exceptions, a web site must notify parents that it plans to collect information from their child and obtain parental consent before it is collected, used, or disclosed. Conditions for more than reasonably necessary information may not be placed on a child's participation in on-line activities. In addition, parents must be allowed to review information collected from the child, to have it deleted, and to prohibit further collection. Finally, companies must implement procedures to protect the confidentiality, security and integrity of personal information collected from children.\textsuperscript{32}

\textsuperscript{31} www.ftc.gov/os/statutes/fcradoc.pdf visited January 19, 2013

5.2.2.4 Financial Modernization Act

More recently, in November 1999, the President signed into law the Financial Modernization Act. The Act's primary purpose was to overhaul the U.S. laws governing the financial services industry, but the legislation also increased the level of financial privacy protections afforded to consumers. The law requires financial institutions to disclose clearly their privacy policies up front and annually, allowing consumers to make informed choices about privacy protection. Financial institutions must also inform consumers if they intend to share or sell consumers' financial data either within the corporate family or to third parties. Consumers are entitled to choice if a financial institution plans to share information with unaffiliated third parties, subject to certain exceptions. Enforcement is allocated among Federal functional regulators (for example, the Office of the Comptroller of the Currency, the Securities and Exchange Commission, and the Federal Reserve Board), the Federal Trade Commission, and State insurance authorities. The legislation directs these agencies to prescribe regulations necessary for its implementation. Regulations have been finalized for all federal regulators. Businesses must be in full compliance by July 2001.

5.2.2.5 U.S. Self-Regulatory Privacy Initiatives

Without broad multi-sector information privacy laws, information privacy protection in the United States has in large part relied on voluntary adoption of self-regulatory codes of conduct by industry. These codes take as their point of departure the same Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data adopted by the OECD as form the basis for the European Directive on Data Protection. As long ago as 1983, 183 U.S. companies endorsed those Guidelines. The U.S. Government has also repeatedly endorsed these guidelines, most recently in October 1998, when the Clinton Administration reiterated endorsement of those Guidelines as part of the Ministerial Declaration on the Protection of Privacy on Global Networks issued at the Ottawa Ministerial Conference.

Recent years have witnessed the growing importance of information privacy in the United States and increasing concern, from both consumers and Clinton
Administration officials, about whether such privacy is sufficiently protected. This concern has led to enactment of additional sector-specific legislation. It has not, however, resulted in any significant movement toward a European type regulatory approach or law. Rather, the emphasis has been primarily on adoption and implementation of more effective self-regulatory regimes to protect privacy or on self-regulation with teeth.

Thus, when in 1997, the Clinton Administration released *A Framework for Global Electronic Commerce*, which examines the policy issues raised by the development of electronic commerce, it noted the growing concerns about information privacy and recognized that, unless they were addressed, electronic commerce would not develop to its full potential. The report specifically recognized the high value Americans place on privacy and recommended private sector efforts and technological solutions to protect privacy. The report also identified several factors suggesting that adopting comprehensive legislation could harm the development of electronic commerce at this time. The lack of national borders on the Internet has heightened interest in self-regulation and technological solutions to problems generally and to privacy concerns specifically. On the Internet, since the issuance of the Clinton Administration's landmark electronic commerce report in 1997, industry has undertaken concerted efforts to create effective privacy protection via self-regulation. More than 80 of the largest companies doing business on the Internet and 23 business organizations that represent thousands of other companies formed the On-line Privacy Alliance (OPA) to promote privacy on-line. The Online Privacy Alliance developed Guidelines for Effective Privacy Policies, which outline protections for individually identifiable information in an on-line or electronic commerce environment. OPA has also produced guidelines for effective enforcement of these policies.

Independent third-party enforcement organizations such as the BBBOnLine, TRUSTe, and CPA WebTrust have also been formed to provide independent third party enforcement regimes that promote compliance with information practice codes. For example, the Council of Better Business Bureaus, a well-regarded, non-profit

---

33 *A Framework for Global Electronic Commerce, 1997*
organization that helps to resolve consumer complaints, established BBB On-Line as a privacy program for online businesses. Businesses joining the program may display a seal or trust mark to notify consumers that their web sites follow fair information practices but only after they adopt privacy policies that comport with the program's fair information practice principles and complete an assessment indicating that they have implemented those policies. Members must also submit to monitoring and review by BBB On Line and agree to participate in a consumer complaint resolution system. The other enforcement programs include similar requirements and also include the display of a seal or trust mark to notify consumers. More than 1950 sites carry a privacy seal from a trusted third party and more than additional 1200 sites have applied for a seal from third-party enforcement services.

In what is perhaps a uniquely American approach to self-regulation, enforcement of self-regulatory programs is backed up by Federal Trade Commission (and other federal and state agency) enforcement. Section 5 of the Federal Trade Commission Act prohibits "unfair and deceptive acts or practices" in or affecting commerce. Deceptive practices have been defined to include representations, omission, or practices that are likely to mislead reasonable consumers in a material fashion. The FTC has repeatedly used its equitable powers under Section 5 to enforce the provisions of privacy (and other self-regulatory) policies against companies failing to comply with the policies they have adopted even where those policies have been adopted voluntarily. The operational effect of these unfair and deceptive statutes is to make adoption by a company of a privacy policy akin to adoption of a privacy law for that particular company.

The FTC Act provides the FTC with authority to seek injunctive relief against future violations of the statute as well as to provide redress for injured consumers. And, the FTC can obtain substantial penalties where its orders are violated. The FTC's (and other federal and state agencies') unfair and deceptive authority and willingness to use this authority to enforce self-regulatory policies helps to ensure the effectiveness of self-regulation in the U.S. All fifty states plus the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have enacted laws similar to the Federal Trade Commission

---

34 The Federal Trade Commission Act
Act to prevent unfair or deceptive acts. These are enforced by their Attorneys General, adding additional resources to government enforcement of self-regulation.

5.3 Information Technology in the European Union

In 1995, the Brussels-based European Union (EU) passed a comprehensive data privacy law called the “European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.” The legislative tool the EU selected for privacy law—the “directive”—requires each EU member state (of which there are now twenty-seven) to enact its own local law adopting (or “transposing”) the thrust of the directive. The EU data Directive mandated that the member states pass their local data laws by October 25, 1998, but in fact full implementation took several years more. Therefore, the text of the EU data Directive offers us a blueprint for data privacy laws across Europe, but in any given situation, the Directive itself is merely a framework. As to each specific data privacy issue arising within Europe, the statute of the relevant country or countries that adopts (“transposes”) the Directive will determine data privacy rights and responsibilities. In other words, the Directive itself speaks only to the twenty-seven member state governments. For most purposes, it does not itself dictate rights of European individuals or companies. But it does serve as a framework for discussing data protection laws across Europe.

5.3.1 The Scope of the Directive

The EU data Directive requires each member state to pass a privacy law, called a “data protection” law that reaches both government and private entities— including

---

36 As of 2007, the European Union consists of 27 member states: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and United Kingdom.
37Directive, ch. I, art. 4 (discussing Member states’ adoption of national provisions).
38Directive, ch. I, art. 4(1).
39Id
businesses that process employee and consumer data. While America's "sectoral" privacy laws target discrete categories of data (medical and credit records, children online, etc.), the Directive mandates omnibus laws that cover all "processing" (defined to include even collection and storage) of data about personally identifiable individuals. The Directive is not anchored to electronic (computerized) data, and therefore reaches written, Internet, and even oral communications. Plus, its sweep goes well beyond business data. Read broadly, the Directive could reach, for example, even private and mundane communications like a love letter or a gossipy chat between friends.40

As computers took over the warehousing of personal data, Europeans' wariness of secret government files morphed into scepticism about corporate databases. A feeling arose that only a coordinated legislative response could protect citizens from abuses of their personal information. In the post-war decades, Europeans took a series of steps in this direction, with some countries (Germany, France) passing their own comprehensive data laws. By 1980, the Organisation for Economic Cooperation and Development (OECD) was able to issue "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data,"41 European Council (not the EU) issued a "Convention for Protection of Individuals with Regard to Automatic Processing of Personal Data."

40 See infra section 24:2.5 The EU data directive could reach a love letter or a gossipy chat because:

- Love letters and gossip tend to contain "information" and "identify" some "natural person"—by definition, "personal data" under Art. 2(a).
- The writing of a letter, or the speaking of gossip, is an "operation . . . such as . . . use, disclosure by transmission, dissemination or otherwise making [personal data] available"—by definition, "processing of personal data" under Art. 2(b) of the Directive. A letter-writer or gossip is a "natural . . . person"—by definition, a "controller" or "processor" of personal data under Directive Art. 2(d), (e).

While presumably European data agencies do not police love letters and gossip, in fact the European data agencies do actively regulate business-context phone calls about fellow workers. See, e.g., Document d'orientation adopté par la Commission le 10 November 2005 pour la mise en oeuvre de dispositif d'alerte professionnelle (French CNIL data agency guidelines of 11/05 on whistleblower hotlines). Some EU member states may have implemented an exception (such as under art. 9) that would except certain love letters or gossip, but even so, the data law would reach, and then possibly except, the love letter or gossip.

41 OECD Council, Sept. 23, 1980

42 Council of Europe, Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, Jan. 28, 1981, European Treaty Series, No. 108; see also Salbu, supra note 8, at 668.
Council conventions were not self-executing, and data protections across Europe continued to vary widely.

Meanwhile, by the 1980s, a reinvigorated European Union was charging ahead, proactively "harmonizing" (aligning) laws across a wide range of sectors as part of its "Single Market Program"—the initiative that solidified a collection of European countries into a single economic entity, the EU. Simultaneously, new technologies were emerging and threatening personal privacy (personal computers, bar code scanning, closed-circuit video monitoring, the Internet, and, more recently, cellular telephones with digital photography).

The EU began examining the impact of technology on society over a fifteen year decade ago; the inquiry culminated in the adoption of a directive in July 1995 specifically addressing information privacy issues. The Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and On the Free Movement of Such Data ("Directive") took effect in October 1998. Member states were required to bring into force laws, regulations, and administrative provisions to comply with the Directive by its effective date. Several have not yet done so.

Presently, six of the fifteen Member States are being sued by the Commission for failure to implement measures within the deadline established by the Directive.43

A quick review of its basic terms makes clear that, consistent with European tradition, the Directive takes an overarching, highly regulatory and inclusive approach to privacy issues. It has two basic objectives: first, to protect individuals with respect to the "processing" of personal information (defined as information relating to an identified or identifiable natural person); and second, to ensure the free movement of personal information within the EU through the coordination of national laws44.

The scope of the Directive is extraordinarily broad. It applies to all processing of data, online and off line, manual as well as automatic, and all organizations holding personal data. It excludes from its reach only data used "in the course of purely personal

44 Article 1 of the European Union Directive.
or household activity. The Directive establishes strict guidelines for the processing of personal information. "Processing" includes any operations involving personal information, except perhaps its mere transmission. For example, copying information or putting it in a file is viewed as "processing." The substantive aspects of the Directive's privacy protections are based on the Guidelines on the Protection of Privacy and trans-border Flows of Personal Data adopted by the Organization for Economic Cooperation and Development (OECD) in 1981.

5.3.1.1 Data Quality

The Directive requires that all personal information must be processed fairly and lawfully, so that, for example, a person whose personal information is at issue knows that it is being collected and used and must be informed of the proposed uses. Furthermore, the use of personal information must be limited to the purpose first identified and to other compatible uses, and no more information may be collected than is required to satisfy the purpose of which it is collected. In other words, the theory is that if a person provides information to obtain telephone service, that information should not be used to target that person for information about vacation trips, nor should information relevant to a customer's interests in vacation trips be required to get, for instance, telephone service. Information must also be kept accurate and up to date.

5.3.1.2 Legitimate Data Processing

The Directive sets forth rules for "legitimate" data processing. Most basically, this requires obtaining the consent of the data subject before information is processed unless specific exemptions apply. In addition, certain information must be provided to data subjects when their personal information is processed, such as whether they have

---

45 Article 3 of the European Union Directive.
46 Article 2 of the European Union Directive.
49 Article 7 of the European Union Directive.
50 Article 10 of the European Union Directive.
rights to see the data, to correct any information that is inaccurate, or to know who will receive the data.\(^{51}\)

### 5.3.1.3 Sensitive Data

"Sensitive" data, such as that pertaining to racial or ethnic origins, political or religious beliefs, or health or sex life, may not be processed at all unless such processing comes within limited exceptions.\(^ {52}\)

### 5.3.1.4 Security

The Directive requires that "appropriate technical and organizational measures to protect data" against destruction, loss, alteration, or unauthorized disclosure or access be taken.\(^ {53}\)

### 5.3.1.5 Data Controllers

The Directive requires those processing data to fulfill very specific requirements. Specifically, they must appoint a "data controller" responsible for all data processing, who must register with government authorities and notify them before processing any data. Notification must at a minimum include: the purpose of the processing; a description of the data subjects; the recipients or categories of recipients to whom the data might be disclosed; proposed transfers to third countries; and a general description that would allow a preliminary assessment of whether requirements for security of processing have been met.\(^ {54}\)

### 5.3.1.6 Government Data Protection Authorities

The Directive also mandates a government authority to oversee data processing activities. Each Member State must establish an independent public authority to supervise the protection of personal data. These "Data Protection Commissions" must have the power to: (1) investigate data processing activities and monitor application of

\(^{51}\) Article 12 of the European Union Directive

\(^{52}\) Article 8 of the European Union Directive

\(^{53}\) Article 17 of the European Union Directive

\(^{54}\) Article 19 of the European Union Directive
the Directive; and (2) intervene in the processing and to order the blocking, erasure, or destruction of data as well as to ban its processing. They must also be authorized to hear and resolve complaints from data subjects and must issue regular public reports on their activities\textsuperscript{55}.

5.3.1.7 Transfers of Data outside the EU

Most importantly from the U.S. perspective, the Directive requires that Member States enact laws prohibiting the transfer of personal data to countries outside the European Union that fail to ensure an “adequate level of [privacy] protection”\textsuperscript{56}. Where the level of protection is deemed inadequate, Member States are required to take measures to prevent any transfer of data to the third country. Member States and their Data Protection Commissions must inform each other when they believe that a third country does not ensure an adequate level of protection.

5.3.2 Determination of Adequacy of Privacy protection under the Directive

The aspect of the Directive that raises major questions for the United States and other non-EU countries is the question of what constitutes an “adequate level of (privacy) protection.” The Directive provides some guidance on how adequacy is to be determined. For example, the Directive states that the adequacy of the protection offered by the recipient country shall be assessed in the light of all the circumstances surrounding a data transfer. These include: (1) nature of the data; (2) purpose and duration of the proposed processing operation; (3) country of origin or the country of final destination; (4) rules of law in force in the destination country and (5) professional rules and security measures that apply within the recipient country\textsuperscript{57}. And, while there seems to be general consensus that “adequacy” means less than “equivalence,” the Directive leaves unspecified the substantive rules that in fact constitute “adequacy” as well as the procedural means for achieving it.

\textsuperscript{55} Article 28 of the European Union Directive
\textsuperscript{56} Article 25 of the European Union Directive
\textsuperscript{57} Ibid
5.4 The UNICTRAL Model Law

The decision by UNCITRAL to formulate model legislation on electronic commerce was taken in response to the fact that in a number of countries the existing legislation governing communication and storage of information is inadequate or outdated because it does not contemplate the use of electronic commerce. The lack of legislation in many countries in dealing with E-commerce as a whole results in uncertainty as to the legal nature and validity of information presented in a form other than a traditional paper document. Inadequate legislation at the national level will inevitably create obstacles to international trade. The purpose of Model law was to offer National legislators a set of internationally accepted rules as to how a number of such legal obstacles may be removed, and how a more secure legal environment may be created for what has become known as electronic commerce. The Model law seeks to permit States to adapt their domestic legislation to developments in communications technology applicable to trade law without necessitating the wholesale removal of the paper-based requirements themselves or disturbing the legal concepts and approaches underlying those requirements. The Model law thus relies on a new approach known as the ‘functional equivalent’ approach which is based on an analysis of the purposes and functions of the traditional paper-based requirement with a view of determining how those purposes or functions could be replaced through electronic commerce techniques.\(^{58}\)

The Drafters of the Model law had considered the impracticability of enacting its entire text as a single statute in all countries. Depending upon the situation in each enacting State, the Model law could be implemented in various ways: either as a single statute or in several pieces of legislation. India opted to enact it as one statute called the ‘Information Technology Act 2000’.

5.5 International Conventions between states

5.5.1 Convention on cybercrime

The Budapest Convention on Cybercrime is the first international treaty seeking to address Computer crime and Internet crimes by harmonizing national laws, improving

investigative techniques and increasing cooperation among nations. It was drawn up by the Council of Europe in Strasbourg with the active participation of the Council of Europe's observer states Canada, Japan and China.

On 1 March 2006 the Additional Protocol to the Convention on Cybercrime came into force. Those States that have ratified the additional protocol are required to criminalize the dissemination of racist and xenophobic material through computer systems, as well as of racist and xenophobic-motivated threats and insults.

The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography, hate crimes\(^{59}\) and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and Lawful interception.

Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

The Convention aims principally at:

1. harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime
2. providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form
3. Setting up a fast and effective regime of international co-operation.

The following offences are defined by the Convention: illegal access, illegal interception, data interference, and system interference, misuse of devices, computer-

related forgery, computer-related fraud, offences related to child pornography and
offences related to copyright and neighbouring rights.

It also sets out such procedural law issues as expedited preservation of stored
data, expedited preservation and partial disclosure of traffic data, production order, search
and seizure of computer data, real-time collection of traffic data, and interception of
content data. In addition, the Convention contains a provision on a specific type of trans-
border access to stored computer data which does not require mutual assistance (with
consent or where publicly available) and provides for the setting up of a 24/7 network for
ensuring speedy assistance among the Signatory Parties.

The Convention is the product of four years of work by European and
international experts. It has been supplemented by an Additional Protocol making any
publication of racist and xenophobic propaganda via computer networks a criminal
offence. Currently, cyber terrorism is also studied in the framework of the Convention.

Its ratification by the United States Senate in August 2006 was both praised and
condemned. The U.S. became the 16th nation to ratify the convention. Forty-three nations
have signed the treaty. The Convention has been signed by Canada, Japan, USA and the
Republic of South Africa on 23 November 2001 (the signing took place in Budapest,
Hungary). Further accessions by other non-European states are planned.

As we have already studied UNCITRAL has hosted a number of conventions on
issues relating to transactions taking place electronically. United Nations Convention on
the Use of Electronic Communications in International Trade was one such convention.
The European Convention establishes basic rules regarding fundamental rights and
liberties that are applicable throughout its Contracting States. The Contracting States
include every EU Member State, as well as numerous other members of the Council of
Europe. Each Contracting State is obliged to ensure that everyone within its jurisdiction,
without regard to nationality or place of permanent residence, enjoys the rights
guaranteed by the Convention. In many Contracting States, these obligations may be
enforced through national courts, on which the Convention is directly binding. To
provide further assurance that the rights will not be abridged, the conduct of Contracting
States is also subject to review by the European Commission on Human Rights and thereafter by the European Court of Human Rights. In addition to the obligations of individual Member States under the ECHR, European Union law also explicitly incorporates the standards set out in the Convention.

Article 8 of the ECHR guarantees the individual’s right to respect for his private and family life. The Article specifies that public authorities may only interfere with this right in narrowly defined circumstances. In particular, any interference must be in accordance with law and necessary in a democratic society, in view of such public interests as national security and the prevention of crime.

These provisions have been interpreted in a series of decisions by the European Court of Human Rights. In these cases, the Court adopts a three-part test for assessing the legality under the Convention of a governmental measure affecting individual privacy:

1) The Court asks whether a right protected by Article 8 has been interfered with;
   It asks whether the interference was in accordance with law. This enquiry requires not only that there be a basis in domestic law for the interference, but also that the legal basis accord with the principle of the rule of law - that it be accessible and that its operation be foreseeable by all citizens;
2) Finally, the Court asks whether the interference was necessary in a democratic society.

The European Court of Human Rights has not previously ruled on a legal challenge to data retention legislation. But the Court has on numerous occasions decided cases involving analogous governmental surveillance of its citizens, frequently finding such regulation to be in violation of Article 8. Analysis of those cases shows that the data retention regime proposed by the draft Framework Decision and now reflected in certain national laws would interfere with the Article 8 right to privacy. Moreover, indiscriminate retention of personal data is not in accordance with law because it fails to distinguish between different classes of people and therefore denies citizens a foreseeable basis on which to regulate their conduct. Finally, such laws are not necessary in a democratic society because blanket retention of data is wildly disproportionate to the law enforcement aims that it seeks to advance.60

60Supra note 42.
5.6 Conclusion

The Information Technology Act is a commendable piece of legislation for India and is a bold step in the right direction. It upholds the spirit of the UNCITRAL Model law. However, it should be borne in mind that the Model law is not intended to cover every aspect of the use of electronic commerce. Hence, there are many more substantive areas that need to be addressed like consumer protection, data protection, spamming, intellectual property, etc. It may be wise to have separate legislation for some of the above rather than complicating the Information Technology Act with numerous things. Similarly, though the provision relating to electronic signatures suited the country's prevailing circumstances and available technology at the time of the legislation, it should be amended in due course in order to accommodate changing technological advances.

There is a myriad of issues that could emanate from the implementation of this legislation. Developing countries generally face the problems of illiteracy, a huge class-divide and infrastructure deficiencies. The technical nature of this law renders it more susceptible to misuse and abuse by the authorities. In some cases, people might not respond to this, again due to ignorance. Hence, proper training of governmental staff and enforcement personnel is vital and should not be neglected. E-commerce has immense potential to generate wealth for developing countries. Enacting legislation in order to facilitate E-commerce transactions is merely a first step. Effective implementation and strategic exploitation of its potential is a much more arduous task and should be done with care and caution. Also, greater attention should be given to promoting electronic governance. The Information Technology Act of India is a laudable work of the Government and it is to be hoped that it will be an inspiration for other developing countries to legislate E-commerce laws as envisaged by the United Nations Resolution on the UNCITRAL Model law. Moreover, these countries will have the advantage of observing and learning from India's experience and taking measures to address some more issues at the enactment stage itself.

61 See Paragraph 13 of the Guidelines to Enactment of the Model Law, supra note 12.