Challenges of Guarding Privacy — Practices Prevalent in Major Countries

Dr. Madan Lal Bhasin

The author is Head, Accounting Department, Mazoon College, Muscat, Sultanate of Oman. He can be reached at madan.bhasin@rediffmail.com

Every electronic transaction — from e-mail and online purchases to medical inquiries and simple surfing — opens you and your data to security and privacy violations. The need for a law relating to privacy protection is increasingly seen in the current era of computer-based networks and cross-border transmission of data, where obtaining and sharing of information on possibly any domain known to man is almost effortless. This article explores the privacy legislation prevalent in US, the European Union, Canada, Japan and India. Privacy laws vary throughout the globe, but unfortunately it has turned out to be the subject of legal contention between the EU and the US. The EU has adopted strict laws to protect its citizens' privacy in sharp contrast to the 'lax-attitude' and 'self-regulated' law of the US. To avoid disruption of business with the EU and possible litigation, US businesses can sign on the "Safe harbor" arrangement. It is expected that a growing number of countries will soon adopt privacy laws to foster e-commerce.

Currently, the only way consumers can stop collection of their personal data is to 'opt-out' or configure the browser to reject 'cookies'. Another method is to use 'Carnivore' program, now called DC$1000. The most noteworthy technique is the W3C Platform for Privacy Preferences (P3P) standard. However, a more reliable way to ensure online privacy is with 'Encryption'. Although encryption software can protect privacy, many governments' forbid the sale or export of strong encryption applications. Moreover, the UK and France still forbid the export, as well as, the use of strong encryption software by their agencies. Today, more advanced technological safeguards are needed. There is no 'single' solution to the erosion of privacy in cyberspace. The battle of privacy must be fought on all the legal, political and technological fronts.

For corporations that collect and use personal information, now ignoring privacy legislative and regulatory warning signs can prove to be a costly mistake. While many experts predict that the US will have strict privacy laws in the near future, for corporations doing business in the European Union countries, the future has already arrived.

The Challenge of Guarding Privacy

Over the last few centuries, human beings have experienced two major revolutions — the industrial revolution and the electronic revolution. The former transformed our society from being agriculture-based to industry-based whereas the latter transformed our society from being mechanical-based to electronic-based. Turban (et al., 2000) observes: "…we are seeing the beginning of a new revolution, namely the network revolution. It interconnects different parts of the world, enabling the seamless flow of information. The Internet is the engine of this revolution and electronic commerce is its fuel." With the introduction of the World Wide Web, electronic commerce has revolutionised traditional commerce and boosted sales and exchanges of merchandise and information.

Today, computers make the collection, maintenance, and manipulation of personal data more possible, faster, less expensive, and more effective than manual methods. A serious concern for individual privacy is growing right alongside the growth of e-commerce. In this context, privacy is the ability of individuals to control information about themselves — what and how much is collected, how it may be used, and so on. Three parties may violate the privacy of individuals — government, businesses, and employers. Governments need individuals' information for planning of infrastructure, education and other services, as well as to facilitate law enforcement. Businesses collect consumer information to better target their marketing and service efforts. Employers monitor employees to ensure productivity and enforce corporate policies. Undoubtedly, all three parties have a legitimate need to collect data on individuals and to

monitor people, but unfortunately their practices threaten privacy. On the other hand, individuals often feel that too many organisations know too much about their private lives. Therefore, many people try as hard as they can to minimise the amount of information collected about them, or at the least, they demand that their consent to use their personal information be obtained.

The origins of data protection can be traced to classical Western notions of an individual's right to privacy and the right to freedom of expression. The belief in protecting an individual's identity and individuality is paramount in some societies. This concept is eloquently stated in the European Convention for the Protection of Human Rights and Fundamental Freedoms—"everyone has the right to respect for his private and family life, his home and his correspondence."

Information relating to individuals, called 'personal data,' is collected and used in many aspects of everyday life. An individual gives personal data when he/she, for example, registers for a library card, signs up for a membership of a gym, opens a bank account, etc. Personal data can be collected directly from the individual or from an existing database. The data may subsequently be used for other purposes and/or shared with other parties. Personal data can be any data that identifies an individual, such as a name, a telephone number, sex, or a photograph.

Advancement in computer technology along with new telecommunication networks has allowed personal data to be carried across continents with ease. The number and nature of infrastructure access devices have multiplied to include: fixed, wireless and mobile devices and a growing percentage of access is through "always on" connections. Consequently, the nature, volume and the sensitivity of information that is exchanged have expanded substantially. The concept of privacy and data protection is especially relevant in the context of the Information Technology Enabled Services (ITeS) segment, particularly the business process outsourcing unit sector.

The Privacy Protection Legislation Scenario

Globalisation is a noteworthy factor behind the increased attention being paid to privacy. To do business around the world, companies have had to adapt to local cultures and regulations. On the surface, it seems obvious that privacy rights should be protected, but the common standard applied differs from country to country. For example, privacy laws in the European Union are much stricter than those in the United States, which implies that US companies who want to do business in the European Union must follow the EU standard. However, the issue is not that simple. Privacy rules, therefore, vary widely throughout the globe, and navigating this thicket of laws is critical to international commerce.

Legislatures all over the world have taken note and tried to minimise invasion of privacy. It is important to state that the laws vary significantly among countries worldwide with respect to protection of citizens' privacy. There are few federal laws in the United States forcing websites to protect the privacy of online users. The two laws deal with the financial/banking industry, in which "opt-out" information must be provided to consumers, and a law protecting the privacy of children. This is why many consumers still fear Web-based shopping. We are summarising below the privacy legislation prevalent in the United States, the European Union, Canada, Japan and India.

The United States

In the US, laws, court rulings and self-regulations govern the protection of an individual's information. While laws now cover financial institutions, in practice, a consumer's privacy is protected primarily by the goodwill of businesses. Most recent privacy concerns have centered on the Internet. Privacy laws in the United States are significantly more lax, especially with regard to non-government organisations. Further, governments are significantly more limited in the collection and dissemination of private data than are private businesses. Law does not limit businesses that are not financial institutions or medical organisations. The US approach has been to expect businesses to impose self-regulation on data collection through the Internet. Whether or not this has happened to any significant degree is questionable. The US government, however, has stepped in despite limitations, and Congress has adopted some laws, as summarised below, to curb violation of privacy.

For corporations that collect and use personal information, now ignoring privacy legislative and regulatory warning signs can prove to be a costly mistake

The Children's Online Privacy Protection Act, 1998: The Children's Online Privacy Protection Act, 1998 (COPPA), which took effect in April 2000, requires online businesses to secure parental consent before collecting personal information from preteen Web surfers. The law makes it a federal offense for commercial websites to collect person-

al information from children under 13, without parental permission. It also forbids release of such information if it has already been collected. To collect information from children, site operators must obtain "verifiable parental consent." This is a problematic point for businesses: How can the consent be verified online? Some jurists suggested that the presentation of a credit card account satisfies the law, because only adults can receive credit cards. Children, however, can use credit card without their parents' permission.

Privacy of Consumer Financial Information Act: The Privacy of Consumer Financial Information Act states that a US financial institution must provide its consumers with a notice of its privacy policies and practices. It prohibits a financial institution from disclosing non-public personal information about a consumer to a non-affiliated third party unless the institution satisfies various disclosures and opt-out requirements, and the consumer has not elected to opt-out of the disclosure. Financial institutions include banks, brokerages, and insurance companies. A "non-affiliated third party" is any organisation that is not owned by the financial institution and any organisation that does not have a business relationship with the consumer.

Companies operating from European Union countries are barred by law from trading with the US companies that do not abide by European privacy laws

Please note here that the organisation must provide an opt-out option, which means if the consumer does not elect to be excluded, the organisation is allowed to transfer his/her personal data to another organisation. US privacy advocates have long required opt-in options. With opt-in, as long as the consumer has not opted to allow the transfer of his/her data, the organisation is barred from doing so. Countries that are members of the European Union enforce opt-in online and offline, because the EU Directive on Data Protection mandates that organisations must receive people's permission to transfer their data to another party.

The European Union

Historically, Europeans have been much more concerned about privacy issues than Americans, and most European countries have enacted very specific and strict laws designed to protect their citizens. The European Union adopted the "Directive on Data Protection (Directive 95)" in October 1998, which limits any collection and dissemination of personal data. In the EU, a directive is framework law; each member nation may legislate a more restrictive law; but not a more relaxed one. The directive imposes the same rules in all 20 countries of the enlarged EU. These countries have passed laws that reflect Directive 95; some are even more restrictive. The Directive provides that no one collects data about individuals ("subjects") without their permission; that the collecting party notify the subject of the purpose of the collection; that the maintainers of the data ask for the subject's permission to transfer the subject's data to another party; and that upon a proper request from the subject, data about the subject be corrected or deleted (see Box-1: European Union Directive on Data Protection). The directive prohibits the transfer of personal data from EU countries to any country that does not impose rules at least as restrictive as those of the directive.

Box-1: EU Directive on Data Protection

It applies to all businesses with operations in European Union countries and those trading with EU countries. Some believe it may also apply to US websites with EU customers.

Protected information:

- Demographics
- Finances
- Health
- Political Affiliation and Political Opinions
- Race or Ethnic Origin
- Religion.

Individual rights:

- To know the protected information possessed by the organisation.
- To have erroneous protected information corrected.
- To "opt-in" to allow the distribution of any "sensitive" information.
- To "opt-out" of the distribution of any protected information for direct marketing purposes.

(The complete text of the EU directive is available at: http://www.privacy.org/oi/intl_orgs/ec/final_EU_Data"_Protection.html)

Companies operating from European Union countries are barred by law from trading with the US companies that do not abide by European privacy laws. To overcome the problem, the US government offered to

create a list of US companies that voluntarily agree to obey these laws. This list is referred to as a "Safe Harbor". A safe harbor is a legal provision that provides protection against prosecution. Now, European businesses have a protection against prosecution if they deal with US businesses that signed up as members of the arrangement. This arrangement is an official agreement between the United States and the European Union. A European company can look up a US business on the list, which is published online, to see if that business participates. US organisations must comply with the seven 'safe harbor principles', as spelled out by the US Department of Commerce (see Box-2: International Safe Harbor Privacy Principles). However, months after the safe harbor was established very few US companies had signed up—by October 2001, the total was only 102 organisations.

The European Union Privacy Directive has important implications both for companies engaged in e-commerce and for multinational corporations with offices in EU countries. It is based on the idea that collecting and using personal information infringes on the fundamental right to privacy. The Directive covers a wide variety of data that might be transmitted during the normal course of business. Although the Directive officially covers only personal data, it defines that to mean "any information relating to an identified or identifiable natural person". Organisations that want to trade in EU countries must guarantee that personal information is processed fairly and lawfully; that it is collected for specified, legitimate purposes; is accurate and up-to-date; and is kept only for the stated purpose and nothing more.

Substantial rights are given to individuals regarding the information that organisations possess about them. Individuals must have access to any personal information collected, and any mistakes must be corrected. More important, individuals may prohibit the use of their personal information for marketing purposes. One recent study suggested that EU Privacy Directive impacts numerous parts of an organisation's records. A partial list of business includes human resources, call centers, customer service, payment systems, sale of financial services to individuals and business, personal and corporate credit reporting, as well as accounting and auditing. All forms of transmission are covered, including electronic and hard copy. In European Union's initial analysis, the US was not listed among those countries seen as adequately protecting the privacy of personal data. Now, almost 250 organisations are

The European Union Privacy Directive has important implications both for companies engaged in e-commerce and for multinational corporations with offices in EU countries

Box-2: International Safe Harbor Privacy Principles

(For Compliance with European Union Privacy Directive)

Notice: An organisation must give conspicuous notice when it collects information, state how it is to be used, and describe the type of third parties to which the information may be disclosed.

Choice: Individuals must be allowed to opt out of whether their personal information is used for other purposes by the organisation and whether it can be disclosed to third parties. For sensitive information, individuals must be given an explicit opt-in choice.

Onward Transfer: An organisation may only disclose to third parties information consistent with the notice and choice principles.

Security: The organisation must establish reasonable security over the personal information gathered.

Data Integrity: An organisation should take reasonable steps to ensure that the personal data collected is accurate, complete, and current.

Access: Individuals must have reasonable access to the personal information complied on them and be able to correct any errors found.

Enforcement: Mechanisms must be established to give individuals recourse if complaints and disputes occur. Penalties must be established for organisations that do not comply with these principles.

The Safe Harbor website is at: http://www.export.gov/safeharbor. The full text is available on the US. Department of Commerce website at: http://www.ita.doc.gov/td/ecom/shorin.html.

on the Department of Commerce's "Safe Harbor" List.

US vs EU Scenario

Transfer of millions of data occurs every day between the US and Europe, and the EU directive gives its member countries essentially "a global reach" with an attached liability for non-compliance. In this context, Greenstein & Feinman (2000) warns US-based international companies: "Basically, non-European companies will have to meet the European Union's directive if they want to conduct electronic commerce in Europe or risk legal action." Thus, international US-based companies may be forced to change their privacy practices in response to laws set abroad.

In the US, the common approach to privacy regulation has been self-enforcement. When the EU put more stringent privacy regulations in place with a Directive on Data and Privacy in 1995, US companies were reluctant to comply. This reluctance came from the knowledge that customer data represents a valuable resource that can be used not only for direct marketing, but also as a separate source of revenue. Businesses in the US commonly sell customer data to other businesses.

Representatives from the United States and the European Union have hammered out a compromise called the Safe Harbor Privacy Principles. Seven principles comprise the framework for the Safe Harbor Privacy Principles. These principles outline requirements for how businesses must inform customers about privacy issues and provide options for them with regard to privacy. In addition, the principles dictate in broad terms how customers data should be secured and access granted, as well as how the guidelines should be enforced.

A major difference between standard practice in the US and EU, including the Safe Harbor Privacy Principles, is in "how individuals may opt-out". In many cases, before sensitive information can be used or discussed to third parties, the organisation must get permission from the individual in an affirmative or explicit opt-in choice. Sensitive infor-

Lamiya Lokhandwala

mation includes medical and health information, information that reveals race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or information concerning the sex life of an individual. Under US rules and practices, US organisations often transfer a great deal of this kind of information without getting opt-in or affirmative permission. US organisations with affiliates operating in the EU need to make sure they are following the stricter EU privacy rules. To understand what is at stake in the EU critical and tangled dispute with the US over privacy, look no further than Daimler Chrysler AG. The giant automaker— the model of the modern multicultural multinational, with one foot planted in Stuttgart and the other in Detroit— deals with an ongoing absurdity. Although the 1998 Daimler-Benz purchase of Chrysler for $37 billion was aimed in no small part at driving international recognition and sales for the combined company's portfolio of brands, information collected about EU customers by the Daimler division (e.g., the demographics of specific Mercedes-Benz car buyers) is generally kept from the Chrysler wing, which might be on the prowl for, say, wealthy German families of four who might be in the market for a Jeep Cherokee. Untold millions of dollars in annual revenues are lost at the iron wall that halts the data flow between the two parts of the company.

Under a 1998 European Union directive, organisations in countries that do not match the Union's privacy standards are, in most cases, prohibited from receiving almost all identification and behavioural data about European Union constituents. With virtually no data protection regulations, the US is one such offender. While the EU and the US seek an agreement, Daimler-Chrysler is cautiously sticking close to the letter of the law. Other US companies echo Daimler Chrysler's approach. For example, Levi Strauss & Company's European headquarters in Brussels deletes consumer-identifying information from e-mail before passing it to the marketing unit in the same building. E-commerce pioneers Amazon.com and eBay have set up Web sites in some European countries that are completely distinct from their American businesses, in part to keep data in the two continents separate. And to sidestep potential prosecution, online advertising company DoubleClick Inc., buffeted by privacy concerns in the US, does not use information tracking software (so called Cookies) in Europe.

Jeffrey Rothfeder narrates the Daimler Chrysler's approach in his book (2001). "Merging two distinct work cultures is difficult enough," says a German Daimler-Chrysler executive involved in the company's privacy initiatives. "But what is perhaps most surprising is the differences in efforts and attitudes among the Germans and the Americans in this company when it comes to the importance of protecting customer information from being misused or customer privacy from being invaded." Disdain for the American view of confidentiality sums up the position of much of the EU, whose 20 countries, by and large, have had stringent privacy laws since the end of World War-II, with especially rigorous rules in Germany, France, and the United Kingdom. This has led to an intractable distance between the EU and US on privacy-protection issues, punctured by marathon, ongoing negotiations over the 1998 Directive that have shown how pronounced the attitudinal and policy differences are between the two regions.

Canada

The Canada passed "The Personal Information Protection and Electronic Documents Act," in 2000. The act provides that Canadians have the right to know why a business or organisation is collecting, using, or disclosing their personal information, such as name, age, medical records, income, spending habits, DNA code, marital status, etc. They also have the right to check their personal information and correct any inaccuracies. According to the act, businesses must obtain the individual's consent when they collect, use, or disclose personal information, except in some circumstances, such as information needed for an investigation or an emergency where lives or safety are at risk.

A major difference between standard practice in the US and EU, including the Safe Harbor Privacy Principles, is in "how individuals may opt-out"

Like members of the European Union, Canada established a privacy commissioner. The privacy commissioner is an officer of Parliament, reporting directly to Parliament. Under the act, individuals may complain to the privacy commissioner about how organisations handle their personal information. The commissioner functions as an ombudsman; initiates, receives, investigates, and resolves complaints; conducts audits; and educates the public about privacy issues. He or She has two sets of powers— the power of disclosure, which is the right to make information public; and the power to take matters to the Federal Court of Canada, which can in turn order organisations to stop a particular practice and award substantial

damages for contravention of the law (Dr. Oz).

The act contains a set of fair information principles. These principles are based on the Canadian Standards Association's Model Privacy Code for the Protection of Personal Information. The code was developed with input from businesses, government, consumer associations, and other privacy stakeholders. The act applies to the collection, use, and disclosure of personal information by organisations during commercial activities both with brick-and-mortar and online businesses. Personal information is any information about an identifiable individual whether recorded or not. Organisations include associations, partnerships, persons, and trade unions. The term "commercial activity" includes the selling, or leasing of donor, memberships, or other fund raising lists.

Japan

Japan also recently passed its first omnibus privacy law, which Professor Alan F. Westin at Privacy and American Business (P&AB) accurately describes as "a 'middle way' between the industry-sector-based privacy laws of the US and the comprehensive data protection laws of the European Union."

India

The fundamental rights, as engrained in the Constitution of India, come closest to protecting an individual's privacy and his freedom of expression. The right to freedom of speech and expression, and the right to privacy are two different sides of the same coin. One person's right to know and be informed, however, may violate another's right to be left alone. Just as the freedom of speech and expression is vital for the dissemination of information on matters of public interest, it is equally important to safeguard the private life of an individual to the extent that it is unrelated to public duties or matters of public interest. The law of privacy, therefore, endeavours to balance these two competing freedoms.

The freedom under Article 19(1)(a) means the right to express one's convictions and opinions freely, by word of mouth, writing, printing, picture, or electronic media. The freedom of expression includes the freedom of propagation of ideas, their publication and circulation and the right to answer the criticism leveled against such views, the right to acquire and import idea and information about matters of common interest. Moreover, a citizen is eligible to safeguard the privacy of his family, marriage, procreation, motherhood, child bearing, education, etc. A citizen's right to privacy is implicit in the right to life and liberty guaranteed under Article 21 of the Constitution, but is subject to the restrictions on the basis of compelling public interest.

The following case law outlines the principles of the law of privacy as prevalent in India.

In *R. Rajagopal v. State of Tamil Nadu*, the Supreme Court was of the opinion that the right to privacy as an independent and distinct concept originated in the field of the court of law. This right has two aspects namely: (a) general law of privacy, and (b) constitutional recognition

given to such right. The right of privacy, however, is not enumerated as a Fundamental Right but has been inferred from Article 21 of the Constitution. Any right to privacy must encompass and protect the personal intimacies of the home, the family, marriage, motherhood etc. In *Mr. X v. Hospital Z*, the Supreme Court was seized on an issue concerning an AIDS patient and the right to privacy and confidentiality regarding his medical condition, and the right of the lady to whom he was engaged to lead a healthy life. The Supreme Court was of the opinion that her marriage and consequent conjugal relations would endanger the life of the fiancée with the AIDS victim, and consequently, she was entitled to information regarding the medical condition of the man she was to marry. In the recent case of *Sharda vs. Dharampal*, the Supreme Court was confronted with the issue whether subjecting a person to a medical test is in violation of Article 21 of the Constitution. The Court outlined the concept of the law of privacy in India and was of the opinion that the right to privacy in terms of Article 21 of the Constitution is not an absolute right. The Supreme Court quoted the previous decision of the same Court in *Govind vs. State of Madhya Pradesh*, where it was held, "Assuming that the fundamental rights explicitly guaranteed to a citizen have penumbral zones and that the right to privacy is itself a fundamental right, that fundamental right must be subject to restriction on the basis of compelling public interest." In conclusion, a citizen is eligible to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child bearing, education, etc.

As regards the state-led initiatives in India, the Andhra Pradesh has proposed a "Data Processing (Special Contracts) Act" in line with the global standards. Accordingly, the Andhra Pradesh Data Protection law seeks to:

- Protect sensitive consumer related information being processed or stored by the BPO/ITES companies or their business associates.
- Provide a data protection and consumer privacy regime similar to the one in European Union, the UK, and the US.
- Enable the companies out locating to AP to enforce their agreements with regard to privacy/protection of sensitive information.
- Provide an avenue for redressal of grievances and resolution of disputes.
- Enable the foreign companies to proceed against their partners/associates in case of violation of privacy rules.

The Andhra Pradesh led initiative is the first of its kind in the country, and a move that will comfort overseas clients as to the privacy concerns over the processing of private data by third-party service players in the state. Most overseas clients protect the privacy of personal data being processed in India by their preferred providers through the traditional contract route.

To sum up, protection afforded to personal data in India may not be considered adequate, as compared to the global standards set by various governments and institutions across the globe. However, there are distinct differences in the concept of privacy that we understand in India vis-à-vis the approach of the Western countries. Generally, Indian society and culture is one of openness, and the concept of protecting one's identity from society is rather alien. However, this is not the position in Western nations, where personally identifiable data

has been widely used to target minorities, fight wars, used for telemarketing purposes, committing financial frauds and scandals, and so on. However, some market players in India have already started misusing the general openness of Indian society to market credit cards, sell personal information, send Spam e-mails, conduct illegal background checks on persons, etc. In this context, it would be necessary to balance the unique nature and needs of Indian society with the privacy and protection principles as expounded by the Indian Constitution.

Will Technology Provide the Privacy Solution?

A program originally called "Carnivore", now called DC$1000, is an e-mail sniffing software that captures data packets passing through Internet service providers (ISPs)

The e-commerce lobby prefers a more 'modest' proposal that would require websites to display a clearly marked box allowing users to "opt-out" of data collection and resale. But it is not clear that "opt-out" proposals would provide meaningful protection for privacy. Moreover, many people seem happy to waive their privacy rights in exchange for free stuff. Currently, the only way consumers can stop the collection of their personal data is to opt out— namely, find the Web page where they can ask the data collector to stop the collection. However, many sites do not do the data collection themselves; they hire companies, such as, DoubleClick to do that for them. Consumers then have to find that third party's site and opt-out. To do so, they have to know that the site they visit contracted with the third party, and many consumers are not aware of the third party's role. No one is eager to inform the public about this, either. As we stated earlier, you can also configure your browser to reject cookies. While this sounds like a good option, it often is impractical. Most cookie-hungry sites are designed to disallow you from browsing further if your computer does not accept cookies. It is a conundrum.

A program originally called "Carnivore", now called DC$1000, is e-mail sniffing software that captures data packets passing through Internet service providers (ISPs). To install the box that runs the Carnivore software at an ISP's site, FBI agents must first obtain a warrant, similar to obtaining a warrant for a wiretap. The software then monitors all transmissions coming from or going to a specific IP address they are targeting. Privacy advocates worry, however, that other e-mail messages could be randomly monitored once the software has been installed at an ISP. As Bowman (2001) observes: "Legislation passed in the Summer of 2001 requires the federal government to reveal how many times law enforcement used DC$1000, the workings of the approval process to use it, and whether it allowed gathering of any unauthorised information."

In the global market various kinds of software are available for privacy protection. For example, Zero-Knowledge Systems Inc. is providing 'privacy and security' bundle of software consisting of Anti-Virus, Anti-Spam, Pop-Up Blocker, Firewall, Parental Control and WebSecure. Freedom WebSecure is a state-of-the-art Internet privacy software (visit www.freedom.net/products for details) that allows for anonymous surfing and private Web browsing. It prevents tracking of your online activities and surfing habits, blocks malicious scripts from the Web pages you visit, shields your IP address and personal information so you can surf anonymously by using 128-bit encryption, neutralizes cookies and active content, removes annoying ads to help speed your Internet connection, and accessible from any computer. ZipLip is a program that encrypts and "shreds" electronic mail. The ZipLip Secure Messaging Suite (visit www.ziplip.com for details) provides a full spectrum of secure messaging solutions enabling any full service institution to securely deliver to all possible touch points. It simply secures delivery and replies, automatic registration and authentication of external users, maintain audit trails for all secure mails, enable secure communications among staff, vendors, customers and partners, etc. Thus, the wide spectrum approach maximises utility, security, and ease of use for all recipients.

KremlinEncrypt is a file encryption program for Macintosh computers (visit www.kremlinencrypt.com for details). Not only does Kremlin feature secure encryption with such algorithms as Blowfish, and RC4, it builds a wall around your computer. When you log off, Kremlin clears sensitive areas of your hard

disk and wipes all records of your activities. It automates the process of securing your computer by scheduling itself to secure portions of your hard disk and all used memory when you log off your computer or computer becomes idle. It can automatically encrypt files and directories when you log off your computer and decrypt them when you log back on, providing a transparent way to protect your files from nosy intruders. You can securely remove files from your computer by dragging them to the secure recycle bin (windows) or secure delete (Mac OS).

Nowadays, some new technological solutions are emerging. The most noteworthy is the World Wide Web Consortium's (W3C) "Platform for Privacy Preferences (P3P)" standard. The P3P is a standardised method for Web sites to encode their privacy policies in a computer-readable format. P3P advocates claim that, with such tools, users can more easily control the use of their personal information. For example, if a site wants to collect data for marketing, under the standard, the user should receive a warning and the option to leave. Users will also see warnings when encountering sites without privacy statements. Such software tools are designed to give Internet users more control over the amount of personal information they disclose online. More information about W3C or P3P is available at www.W3.org. Microsoft's Internet Explorer 6 browser was the first consumer software to incorporate P3P. But P3P will only work if most websites voluntarily participate. In addition, the Electronic Privacy Information Center (EPIC) issued a critical report in 2000 titled "Pretty Poor Privacy," where it called for further improvements in P3P.

Another way to ensure online privacy is with Encryption— conversion of data into a secret code. When conducting e-business transactions and sending credit card information online, for example, encryption can protect the user from theft of information that can lead to fraud. The most common foolproof way to prevent someone from reading your e-mail is to use software to encrypt it, thus, rendering it incomprehensible to anyone without the decoder (or key). There are two major commercial encryption standards in use: Pretty Good Privacy (PGP) and Secure Multipurpose Internet Mail Extensions (S/MIME). The PGP is relatively easy to install (available free to non-commercial users, visit www.mcafreesecurity.com/us/products/home.html) and configure, and widely accepted tool. Like a safe-deposit box, it uses two keys—one 'private' and one 'public'—only its keys are complex electronic passwords. To read a PGP-encrypted message, you need both keys. On the other hand, S/MIME is also available free on the Internet and is included in the Netscape Navigator and Microsoft Internet Explorer browser packages. It is available as a 'plug-in' to most e-mail packages. However, S/MIME is simple to configure and use—with two major exceptions. S/MIME uses a shorter code for its key, making it easier for a hacker to crack, and S/MIME does not rely on public keys; instead it uses third-party authentication relying on digital certificates.

However, one advantage of PGP over S/MIME is its acceptance rate. Since PGP is widely used encryption software package, compatibility is hardly an issue. Additionally,

it can be plugged into the most popular e-mail software applications. However, PGP and S/MIME can detect message tampering by using their digital signature features. PGP's digital signature software applies an algorithm (or formula) to the message content that automatically generates a unique code, or digital signature. Thus, encryption enables authentication and confidentiality in communication over computer networks.

The US has adopted Secure Hash Algorithm (SHA) and allowed its own citizens to use such encryption schemes, but removed encryption techniques from its list of controlled export items only in the late 1990s. "As a simmering undercurrent to the privacy discussions, the US' stubborn stance against exporting strong encryption software unless American security agencies are allowed access to the keys has added to worries in Europe that some US companies are using data surveillance technology for industrial espionage, giving them an unfair advantage in bidding for lucrative industrial and defense contracts. That possibility (and some Europeans believe there is evidence to support it) has made EU member governments even more antagonistic to giving in to the US on any data protection issue," asserts Jeffrey Rothfeder. However, the United Kingdom and France still forbid the export as well

There are two major commercial encryption standards in use: Pretty Good Privacy (PGP) and Secure Multipurpose Internet Mail Extensions (S/MIME)

as the use of strong encryption software by their agencies.

The Future Scenario and Prospects

Companies are entering an era of information transparency of increasingly activist stakeholders, the growing influence of global markets, the spread of communications technology, and a new customer ethic demanding openness, honesty and integrity from companies. Consequently, risks to privacy are greater, and safeguarding sensitive information has become more significant, and more difficult to do. Among the companies who are given high marks by privacy advocates for making data protection a priority are Dell, IBM, Intel, Microsoft, Procter & Gamble, Time Warmer and Verizon. Some of these companies— such as Microsoft, which has in the past been plagued by security leaks in its operating system and e-commerce programs— have embraced hard-line privacy stances only after experiencing first-hand the potential damage to their businesses that privacy breaches can inflict.

One advantage of PGP over S/MIME is its acceptance rate. Since PGP is a widely used encryption software package, compatibility is hardly an issue

Over the past few years, dozens of bills concerning the protection of privacy have been introduced at both the federal and state levels. Recently, Microsoft has launched a project in 2004 called "Trustworthy Computing," under which Chairman Bill Gates has challenged the company "to be certain that availability, security, privacy and trustworthiness are key components of every software and service product the company develops."

Although many US companies initially fought consumers' efforts to make companies pay attention to privacy, almost no major businesses today feel they can completely neglect data protection rules. Thus, all businesses must now take consumer privacy seriously. This will require investing resources to secure databases and websites. Organisations should also determine if their insurance covers lawsuits that may arise over privacy violation issues. In the very near future, all organisations with an online presence will need to establish online privacy statements or policy certifying that they comply with legislated privacy standards. US corporations, with operations in the EU, must comply with the EU Privacy Directive through the use of the 'Safe Harbor Agreement'. Ignoring these rules might put a US Corporation in the awkward position of not being able to access its own records from the EU, either in electronic or hard copy form. While many predict that the US will have strict privacy laws in the near future, for corporations doing business in European Union countries, the future has already arrived!

The protection afforded to personal data in India may not be considered adequate, as compared to the global standards set by various governments and institutions across the globe. There is no single solution to the erosion of privacy in cyberspace. The battle of privacy must be fought on many fronts— legal, political, and technological—and each new assault must be vigilantly resisted as it occurs. ❐