RIGHT TO PRIVACY
AND
DATA PROTECTION

Nishith Desai Associates
Legal & Tax Counselling Worldwide

93-B MITTAL COURT, NARIMAN POINT
MUMBAI 400 021. INDIA
TEL: 91 (22) 282-0609
FAX: 91 (22) 287-5792

220 CALIFORNIA AVENUE., SUITE 201
PALO ALTO, CA 94306, USA
TEL: 1 (650) 325-7100
FAX: 1 (650) 325-7300

nda@nishithdesai.com
www.nishithdesai.com

This paper is a copyright of Nishith Desai Associates. No reader should act on the basis of any statement contained herein without seeking professional advice. The authors and the firm expressly disclaim all and any liability to any person who has read this paper, or otherwise, in respect of anything, and of consequences of anything done, or omitted to be done by any such person in reliance upon the contents of this paper.

For Private Circulation Only

RIGHT TO PRIVACY AND DATA PROTECTION

Aashit Shah and Nilesh Zacharias
Nishith Desai Associates

Nishith Desai Associates ("**NDA**") is a research based international law firm based in Mumbai and Palo Alto, Silicon Valley, specializing in information technology, e-commerce, telecommunications, media and entertainment laws, international financial and tax laws and corporate and securities laws. It has acted as strategic and legal counsel to premier corporates in their Internet forays, including IL&FS, GE Capital, Jasubhai Group, software majors such as i2 Technologies, Mahindra British Telecom and communication companies such as Space Systems/Loral, New Skies Satellite, Flag and WorldTel. Apart from structuring and acting for a large number of private equity funds in India, NDA has been involved in American Depositary Receipt (ADR) offerings of Indian companies, representing Wipro, Rediff.com and Silverline Technologies and acting as underwriter's counsel in Infosys Technologies and Satyam's ADR offerings. NDA was involved in the first cross-border stock swap merger from India - BFL's acquisition of MphasiS besides Silverline's recent acquisition of Seranova Inc in an ADR stock swap deal. It has also advised the Government of India and Internet Service Providers Association on e-commerce issues in the WTO regime. It represented NASSCOM at a Joint WTO-World Bank Symposium on Movement of Natural Persons held in Geneva in April 2002. NDA was recognized as the "I**ndian Law Firm of the Year 2000**" and "**Asian Law Firm of the Year 2001 (Pro Bono)**" by the International Financial Law Review, a Euromoney Publication. It has also been ranked as having a l**eading practice in Private Equity, Media and Entertainment and IT and telecommunications law** for 2001-02 by the Global Counsel 3000.

© Nishith Desai Associates 2001

RIGHT TO PRIVACY AND DATA PROTECTION

Aashit Shah and Nilesh Zacharias
Nishith Desai Associates

Synopsis

Introduction

Immense concerns are already prevailing with respect to the protection of personal data and information, in essence the right to one's privacy. The right to privacy refers to the specific right of an individual to control the collection, use and disclosure of personal information. Personal information could be in the form of personal interests, habits and activities, family records, educational records, communications (including mail and telephone) records, medical records and financial records, to name a few. Further, the convergence of technologies has spawned a different set of issues concerning privacy rights and data protection. Innovative technologies make personal data easily accessible and communicable. Predictions by the Forrester Research Institute in 2001 indicated that as much as US$15 billion worth of the projected e-commerce revenues would be lost by online retailers in 2001 because of customers' privacy concerns.[1]

This basic right to protect an individual's privacy has been enshrined in the Universal Declaration of Human Rights, 1948[2] ("**UDHR**") as follows:

"Article 12: *No one shall be subjected to arbitrary interference with his privacy, family, home* or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

[1] "Forrester Research: Privacy issues inhibit online spending" http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905357259&rel=true (As visited on April 19, 2002)
[2] India is a signatory to the UDHR.

© Nishith Desai Associates 2001

This human right has also been articulated in the International Covenant on Civil and Political Rights, 1976[3] ("**ICCPR**"). The obligations imposed under the ICCPR require the State to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right.[4] The UDHR and the ICCPR are directly binding upon India as it is a signatory to both these international conventions. However, no consequent legislation has been enacted in India to protect this coveted right.

Indian Legal Scenario

Constitution of India

The right to privacy has been interpreted as an unarticulated fundamental right under the Constitution of India ("**Constitution**"). The growing violation of this right by the State on grounds (that are not always bona fide) encouraged the Indian Judiciary to take a pro-active role in protecting this right.

A landmark judgment with respect to this issue is *Kharak Singh v. State of U.P.*[5] The Supreme Court held that the right of privacy falls within the scope of Article 21 of the Constitution and therefore concluded that an unauthorized intrusion in to a persons home and disturbance caused to him is in violation of personal liberty of the individual.

However, in *Gobind v. State of Madhya Pradesh*,[6] the Supreme Court qualified the right to privacy and held that a violation of privacy could be possible under the sanction of law.

The scope and ambit of the right of privacy or right to be left alone came up for consideration before the Supreme Court in *R. Rajagopal v. State of T.N.* during 1994.[7] In this case the right of privacy of a condemned prisoner was in issue. By interpreting the Constitution in light of case law from the United Kingdom ("**UK**") and United States ("**US**"), Justice B.P. Jeevan Reddy held that though the right to privacy was not enumerated as a fundamental right, it could certainly be inferred from Article 21 of the Constitution.

Another significant case related to the right of privacy was the *People's Union of Civil Liberties v. the Union of India*.[8] The case was primarily involved with the issue of 'telephone

---

[3] India is a signatory to the ICCPR.

[4] http://www.unhchr.ch/tbs/doc.nsf/(symbol)/CCPR+General+comment+16.En?OpenDocument (As visited on July 17, 2001).

[5] AIR 1963 SC 1295. In this case, it was held that the expression "right to life" was not limited to bodily restraint or confinement to prison only but something more than mere animal existence. Here the Petitioner was kept under police surveillance, while he was charged with the offence of dacoity. The police made domiciliary visits to his house for verification of his movements and activities.

[6] (1975) SCC (Cri) 468. The case related to surveillance according to Regulations 855 and 856 of Madhya Pradesh Police Regulations. The Court held that though the right to privacy existed, it had not been violated since the procedure was required by law.

[7] Auto Shankar, a condemned prisoner, wrote his autobiography while confined in jail and handed it over to his wife for being delivered to an advocate to ensure its publication in a certain magazine edited, printed and published by the petitioner. This autobiography allegedly set out close nexus between the prisoner and several officers including those belonging to IAS and IPS some of whom were indeed his partners in several crimes. The publication of this autobiography was restrained in more than one manner. It was on these facts that the petitioner challenged the restrictions imposed on the publication before the Supreme Court.

[8] (1997) 1 SCC 318. In this case, Section 5 (2) of the Indian Telegraph Act, 1885 was challenged since it allowed the concerned authorities to intercept message for transmission by or transmitted or received by any telegraph, in the interests of national sovereignty. The decision in this case was a result of a broad interpretation of Article 21 of the Constitution, thereby including telephone tapping as a violation of privacy.

© Nishith Desai Associates 2001

tapping' and held that tapping a person's telephone line violated his right to privacy, unless it was required in the gravest of grave circumstances such as public emergency.[9]

While it may seem that the right to privacy is adequately protected as a fundamental right, it is essential to keep in mind that barring a few exceptions, fundamental fights secured to the individual are limitations only on State action. Thus, such an interpretation will not protect an individual against the actions of private parties.

Law of Torts

Common law principles of torts do not provide direct action for invasion of privacy. The law of torts seeks to provide protection by the use of civil wrongs such as defamation, trespass and breach of confidence. However, with the advent of new technologies, such common law seems manifestly unsuited to this new environment. The need is for a specific enactment to deal with privacy and data protection issues.

The Information Technology Act, 2000 ("ITA")

The ITA was enacted to provide a comprehensive regulatory environment for e-commerce. In connection with the right to privacy on the Internet, it is pertinent to examine Section 69 and Section 75 of the Act. Section 69 is similar to the provision of Section 5 (2) in the Indian Telegraph Act, 1885 and empowers the Controller[10] to direct any agency of the Government to intercept any information transmitted through any computer resource, and requires that users disclose encryption keys or face a jail sentence upto 7 years. Section 72 on the other hand is the only express provision in the act connected with privacy and breach of confidentiality. It provides that any person who discloses the contents of any electronic record etc. without the consent of the person concerned shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

However, both the provisions in the Information Technology Act, 2000 deal specifically with the powers of the Government in connection with the privacy of individuals.

From an understanding of the Indian legal scenarios, it can be concluded that there exists no Indian legislation that covers the protection of rights of privacy, which can be interpreted in the realm of transactions between individuals and corporations or between two individuals over the Internet.

International Developments

In the international sphere, there have been several developments to protect the right to privacy.

---

[9] Shyamkrishna Balganesh and Niranjan Maitra,"Cryptography, Privacy and National Security Concerns" Law Relating to Computers, Internet and E-commerce, 2nd Edn., 2001, p. 377.

[10] Section 2 (m):"Controller" means the Controller of Certifying Authorities appointed under sub-section (I) of section 17 [Information Technology Act, 2000].

© Nishith Desai Associates 2001

United Nations

Besides the UDHR and ICCPR, the UN Convention on Protection of the Child and the Convention for the Protection of Human Rights and Fundamental Freedoms, 1950[11] also contain provisions for the protection of privacy rights.

Organisation for Economic Co-operation and Development ("OECD")

The OECD[12] has formulated Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("**the Guidelines**"), which state that 'the development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data'.[13] The Guidelines attempt to balance the protection of privacy and individual liberties and the advancement of free flows of personal data through eight privacy principles which, if observed, are supposed to guarantee a free flow of personal information from other OECD countries. However, the Guidelines are not legally binding and on the whole the Guidelines constitute a general framework for concerted action by Member countries: objectives put forward by the Guidelines may be pursued in different ways, depending on the legal instruments and strategies preferred by Member countries for their implementation.

Although the Guidelines are being increasingly used as the world standard some critics maintain that the Guidelines should be revised in light of technological change and developments in the collection and use of personal information. It has been suggested that additional data protection principles are needed such as the right not to be indexed and a right to encrypt personal information effectively.[14] Although the OECD Guidelines were developed in 1980, they continue to represent an international minimum standard for privacy protection. As well, the Guidelines have been the basis of or have strongly informed the data protection legislation of most OECD Member States.

India is not a member of the OECD, but in the year 2001 it became the 27th member of the Development Centre, a semi-independent body within the OECD that works to foster policy dialogue and understanding between OECD countries and the developing world.

European Union

The European Parliament and the Council of the European Union passed the Data Protection Directive with an aim to establish a regulatory framework to protect privacy through meeting three stated objectives.

---

[11] Article 8.

[12] http://www.oecd.org . The OECD is an organization that provides governments a setting in which to discuss, develop and perfect economic and social policy. They compare experiences, seek answers to common problems and work to co-ordinate domestic and international policies that increasingly in today's globalised world must form a web of even practice across nations.

[13] For the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data refer to: http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM (As visited on April 18, 2002).

[14] Kirby, Michael D "Privacy Protection – a New Beginning" *21st International Conference on Privacy and Personal Data Protection - Conference Proceedings* 5. Available at: www.pco.org.hk/conproceed.html (As visited in July 2001).

© Nishith Desai Associates 2001

The objectives are:

- to protect the rights and freedoms of individuals regarding the processing of personal data;
- to harmonize data protection standards throughout Europe; and
- to limit movement of data to those countries outside of Europe that do not have adequate levels of protection.[15]

The Directive aimed at facilitating the development of electronic commerce by fostering consumer confidence and minimizing differences between member states' data protection rules. The directive requires E.U. member states to adopt national legislation ensuring privacy protection if they wish to participate in the free flow of information within the European Union. Under the Directive, data subjects[16] are granted a number of important rights and may appeal to independent national authorities, if they consider their rights are not being respected.

One provision of the directive which caused much uncertainty in the international business community, especially the US was Chapter IV- "Transfer of Personal Data to Third Countries'. Article 25, which establishes the general rule is that data should only be transferred to a non-EU country if they will be adequately protected there. However, the directive failed to define "adequate." Instead, it provided that adequacy determinations will be made on a case-by-case basis, taking into account all the circumstances surrounding a data transfer operation. The provision in Article 25 is compatible with the General Agreement on Trade in Services (GATS, Article XIV), which recognises the protection of personal data as a legitimate reason for restricting the free movement of services. Because of the unclear impact of the "adequacy" standard on personal data transfers from the EU countries to US, which did not have an Act protecting privacy of all personal data transfers or an agency which monitored security of personal data, the US would be 'inadequate' by European standards.

United States

The Privacy Act of 1974[17] protects records held by US Government agencies and requires them to apply basic fair information practices. Like the Indian Constitution, there is no explicit right to privacy in the US Constitution. However, US Courts have interpreted the right to privacy to be included in the US Constitution.

The US has no comprehensive privacy protection law for the private sector. A patchwork of federal laws covers some specific categories of personal information.[18] These include financial records,[19] credit reports,[20] video rentals,[21] cable television,[22] children's (under age 13) online activities[23] educational records,[24] motor vehicle registrations,[25] and telephone

[15] Refer to the EU Directive on Data Protection: http://www.doc.gov/ecommerce/eudir.htm
[16] Article 2 (a) 'personal data' shall mean any information relating to an identified natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
[17] http://www.epic.org/privacy/laws/privacy_act.html (As visited on April 16, 2002).
[18] Marc Rotenberg, The Privacy Law Sourcebook, EPIC 1999: http://www.epic.org/bookstore/pls
[19] Right to Financial Privacy Act.
[20] Fair Credit Reporting Act, PL 91-508, amended by PL 104-208 (Sept. 30, 1996). http://www.ftc.gov/os/statutes/fcra.htm.
[21] Video Privacy Protection Act of 1988.
[22] Cable Privacy Protection Act of 1984: http://www.epic.org/privacy/cable_tv/ctpa.html (As visited on April 16, 2002).
[23] See Center for Media Education, A Parent's Guide to Online Privacy: http://www.kidsprivacy.org/ (As visited on April 16, 2002).

records.[26] However such activities as the selling of medical records and bank records, monitoring of workers, and video surveillance of individuals are currently not prohibited under federal law. There is also a variety of sectoral legislation on the state level that may give additional protections to citizens of individual states.[27] The tort of privacy was first adopted in 1905 and all but two of the 50 states recognize a civil right of action for invasion of privacy in their laws.

An important step taken in the US towards the protection of privacy on the Internet was the enactment of Children's Online Privacy Protection Act (COPPA).[28] Under the rule, commercial Web sites and online services directed to children under 13 or that knowingly collect information from them must inform parents of their information practices and obtain verifiable parental consent[29] before collecting, using, or disclosing personal information from children.

International Safe Harbour Principles

There was a need to diminish the divide between the United States and the European Community who adopted different approaches to privacy protection to their citizens. Following extensive discussions, the EU Working Party and the U.S. Department of Commerce agreed that the department would compile a publicly accessible list of companies that provide adequate protection for personal data. Companies and individuals that subscribe to certain safe harbor principles will be able to secure protection against future data blockages

The agreement between the European Union and the United States rests on seven safe harbor principles: notice, choice, onward transfer, security, data integrity, access and enforcement. India could incorporate these principles while formulating legislation in this behalf.

Other countries

Several other countries such as UK, Spain, Switzerland, Sweden, Australia, China (Taiwan), Thailand, Singapore, to name a few, have enacted laws to protect data and privacy rights.

Alternatives Available to India

Modes of Regulation

Considering that the international community regards the right to privacy and data protection as a basic human right, India may be under a moral as well as legal obligation to enact

---

[24] Family Educational Rights and Privacy Act, 1974: http://www.epic.org/privacy/education/ferpa.html (As visited on April 16, 2002).
[25] Drivers Privacy Protection Act, PL 103-322, 1994: http://www.epic.org/privacy/laws/drivers_privacy_bill.html (As visited in July 2001).
[26] Telephone Consumer Protection Act, 1991.
[27] Compilation of State and Federal Privacy Laws (1997 ed.), by Robert Ellis Smith and Privacy Journal. http://www.epic.org/privacy/consumer/states.html (As visited on April 16, 2002).
[28] http://www.cdt.org/legislation/105th/speech/copa.ht (As visited on April 16, 2002).
[29] Verifiable parental consent is defined as "any reasonable effort (taking into consideration available technology) ... to ensure that a parent of a child ... authorizes the collection, use, and disclosure" of a child's personal information."

© Nishith Desai Associates 2001

privacy and data protection regulations. There are two modes in which regulations can be adopted: Self-regulation and Government regulation

- *Self-regulation* - India could consider promoting an initiative among Indian industries, especially those interested in the growth of e-commerce. Self-regulation by the industry offers the advantage of a flexible policy made by those who know the trade practices and are motivated by the desire of customers. Self-regulation is also cost efficient to the government, as enforcement mechanisms need not be established. However, a large and heterogeneous group of agents may make self-regulation difficult. However, there is also the risk that self-regulatory solution would be to set the lowest standard.

- Government Regulation - Alternatively, the Indian government could adopt specific legislation to address privacy and data protection issue. Even countries like the US that have primarily taken a self-regulatory approach to protecting privacy on the Internet, are slowly moving towards Government regulation to bring about uniformity and effective application of privacy standards.

Issues to be considered

Enumerated below are some of the issues that the Indian Legislature should try to keep in mind while drafting a privacy law.

- *Protection from arbitrary and unlawful interference: by the Government and private parties*– The legislation must ensure that an individual's right to privacy is not interfered with in an arbitrary and unlawful fashion. Presently, judicial precedents prohibit violation of the right to privacy of an individual by Government agencies. A comprehensive law must provide for protection from intrusion by the Government as well as private parties.

The law must also address issues relating to trespass upon individual privacy, audio and video surveillance and interception of communications (including digital and electronic communications).

It must also try and prohibit/curtail the use of cutting-edge technology to trespass upon privacy rights and personal data. Presently, the right to privacy on the Internet is being threatened due to several elements such as web cookies, [30] unsafe electronic payment systems, [31] Internet service forms,[32] browsers[33] and spam mail.[34]

---

[30] http://www.cookiecentral.com/faq/. A Cookie is a message given to a Web browser by a Web server. The browser stores the message in a text file called *cookie.txt*. The message is then sent back to the server each time the browser requests a page from the server. Cookies were initially designed to address the fact that Web sites didn't know whether a user is a first time or repeat visitor, and possibly prepare customized Web pages for them. The information placed in a cookie is not only useful in the context of e-commerce but cookies provide marketing information; they can track the ads that have been clicked on, in order to provide internet users with similar banner ads in the future. Cookies are a source of concern relating to privacy on the Internet, because of the ability to track the activities of users without their knowledge.

[31] While purchasing anything on the Internet a consumer is required to use a credit card. This results in the transmission of a credit card number over the Internet, which is very sensitive personal data and the concern is that this information will then be re-used for another purpose or sold to direct marketers. Consumers are three to four times more likely to experience theft or misuse of their credit cards when they shop online. ('Jupiter Media Metrix report on e-commerce fraud' by Jim Van Dyke) Part of the problem is that some web site owners don't understand how to secure their sites properly or how to hire skilled staff, or they lack the funding necessary to provide adequate security measures to ensure privacy protection.

[32] While subscribing to most Internet services, or gaining membership to online clubs Web sites require visitors to provide some extremely personal information, without offering any assurance with regards to privacy of that information. To join, users are

- *Protection of medical records* – Historically, medical records were used largely by physicians and medical insurers. However, with the creation of electronic records and large databases of medical information, the number of health care professionals and organizations with access to medical records has increased. While such availability allows for research that can improve the understanding of diseases and treatments across broad populations, the number of parties with routine access to personally identifiable medical data has raised concern about the potential misuse of this data.[35] It is essential that such data is not collected and sold to researchers in the field biomedical science, without the consent of the patients. With the advent of the internet, it has become increasingly difficult to track such data and not only does it amount to an invasion of privacy, but it also amounts to breach of the duty of confidentiality that medical professionals owe their patients

- *Protection of financial records* – Financial records of individuals must also be protected from being distributed and circulated among banks and financial companies as it may also result in the misuse of such information.

- *Preventing excessive monitoring of employees by the employer* – Another major concern, especially among the working class is the excessive surveillance of employees activities by their employers. Recently, Privacy Foundation, a non-profit group in the US, reported that about 100 million workers, or about 27 percent, are subject to continuous surveillance of their e-mail and Internet use.[36] This is an issue of rising importance and must be dealt with in a comprehensive manner.

Principles that could be adopted

These principles are based on the Safe Harbour Principles adopted between EU and US.

- *Notice* - The data subject must be given notice in clear language, when first asked for personal data, of the purpose of data collection, the identity of the data controller, the kinds of third parties with whom the data will be shared, how to contact the organization collecting or processing the data, and the choices available for limiting use or disclosure of the information.

---

almost always required to give their name, address, telephone number, e-mail address, products bought etc. The primary purpose of gathering personal information about consumers is market research. The information collected helps online businesses to understand consumer trends and helps them target their consumers more effectively. This personal information is either used by the business collecting it or is often sold to other businesses with a view to getting direct access to the consumers they wish to target.

[33] An Internet Browser interprets HTML the programming language of the Internet, into the words and graphics that are seen my Internet users when viewing a web page. It is a type of software that allows Internet users to navigate information databases. There have been many reports of security bugs in browsers, which can enable web sites to access your personal information while a person is surfing the web. Most manufactures of Internet browsers have attempted to fix the bugs to prevent access to sensitive personal data of the users of such browsers. However, the threat still persists and browsers could result in the leakage of information such as the e-mail address or username of the Internet user. To understand how browsers leak information to http servers refer to http://www.cen.uiuc.edu/~ejk/WWW-privacy.html.

[34] Spam is the use of e-mail addresses for a purpose that consumers have not consented for and constitute a violation of personal rights. Internet users who have purchased a product over the Internet or have their e-mail address published on a web site or have subscribed to a news service or who have participated in news groups or mailing lists, often receive unsolicited / spam e-mail. Some Internet Service Providers and other Internet businesses engage in the unlawful practice of selling lists of their customer's e-mail addresses to other companies. These companies use programs to generate bulk e-mail messages that are intended to advertise or promote a business, web site or product.

[35] "US Report to Congressional Requesters on Medical Records Privacy" www.epic.org/privacy/medical/gao-medical-privacy-399.pdf (As visited in July 2001).

[36] http://news.cnet.com/news/0-1003-202-6477622.html (As visited in July 2001).

- *Choice* - The data subject must be given clear, affordable mechanisms by which he or she can opt out of having personal information used in any way that is inconsistent with the stated purposes of collection.

- *Onward transfer* - Where the data controller has adhered to the principles of notice and choice, it may transfer personal data if it ascertains that the receiving party also complies with the safe harbor principles, or if it enters into a contractual agreement that the receiving party will guarantee at least the same level of data protection as the transmitting party. When disclosure is made to a third party that will perform under instructions of the data controller, it is not necessary to again provide notice or choice, but the onward transfer principle continues to apply.

- *Security* - The data controller must take reasonable precautions to protect data from loss or misuse, and from unauthorized access, disclosure, alteration or destruction.

- *Data integrity* - The data controller must take reasonable steps to ensure that data are accurate, complete and current.

- *Access* - Data subjects must have reasonable access to their personal data and an opportunity to correct inaccurate information.

- *Enforcement* - At a minimum, enforcement mechanisms must include readily available and affordable recourse for the investigation of complaints and disputes, damages awarded where applicable, procedures for verifying the truthfulness of statements made by the data controller regarding its privacy practices, obligations of the data controller to remedy problems arising out of noncompliance, and sanctions sufficiently rigorous to ensure compliance.

Conclusion: Urgent Need for Privacy Regulations

Keeping in mind the growth and implications of international trade, especially with the influence of the Internet, it is imperative that India cooperate with the world community to establish laws strictly pertaining to protection of privacy and personal data. Currently countries (eg. EU countries) are unwilling to trade with India due to inadequate privacy regulations. This is particularly relevant, as India becomes an outsourcing center for several back-office operations such as credit processing, medical transcription, et al. The threat of privacy is also an obstacle towards facilitating a secure environment for communication over the Internet. Unless these issues are addressed India cannot take full advantage of the tremendous opportunities and benefits that e-commerce presents to developing nations such as ours.

A legal framework needs to be established setting specific standards relating to the methods and purpose of assimilation of personal data offline and over the Internet. Consumers must be made aware of voluntarily sharing information and no data should be collected without express consent. The future of India's trade depends on striking an effective balance between personal liberties and secure means of commerce.

© Nishith Desai Associates 2001