DATA PRIVACY, DATA PIRACY:

CAN INDIA PROVIDE ADEQUATE PROTECTION FOR

ELECTRONICALLY TRANSFERRED DATA?

DATA PRIVACY, DATA PIRACY: CAN INDIA PROVIDE ADEQUATE PROTECTION FOR ELECTRONICALLY TRANSFERRED DATA?

Vinita Bali

I. INTRODUCTION

Three employees of Mphasis, a business process outsourcing ("BPO") firm which runs call center services for Citibank's US customers in Bangalore, India, were arrested for allegedly siphoning $350,000 from the accounts of Citibank's US customers. These employees used their position which provided them access to Citibank customers to induce four of them into giving out the personal identification numbers to their accounts, allowing the employees to illegally siphon funds out of the customers' accounts.[1] Outsourcing is a growing trend among budget-conscious U.S. companies and institutions. Information being outsourced includes personal data and confidential, proprietary information. For example, Unisys Corp., a company that handles sensitive information such as police records and databases for the US Department of Homeland Security, is among scores of big corporations that farm out technology-related work to economically

[1] While Mphasis maintained that its security procedures, especially detection and enforcement systems, were adequate, industry analysts warned that this incident could heavily impact the offshoring industry in India. Forrester Research, a US publicly traded independent technology and market research company that focuses on the business implications of technology change, stated that the breach would have "far-reaching" negative connotations for the offshore BPO industry and said that the high turnover of Indian call centre staff makes it increasingly difficult to adhere to security processes and sufficiently check backgrounds. A Forrester research note said: "While the center in Pune was BS 7799 (security certification) and CMM Level 5 (quality certification) certified, the breach still occurred. Clients and prospects should not be lulled into security complacency by the laundry list of certifications or process changes that suppliers roll out. Customers are going to have to implement their own aggressive requirements, such as eliminating writing instruments in their offshore centers and auditing bi-monthly to ensure that the vendor is following mandated processes."Forrester also claimed offshore call centre growth could drop by as much as a third because of security concerns, regulatory pressure and a consumer backlash. Andy McCue, *Indian Call Centre Staff in $350,000 Citibank Theft*, SILICON.COM, April 11, 2005, *available at* http://www.silicon.com/research/specialreports/offshoring/0,3800003026,39129426,00.htm (last viewed November 30, 2005).

efficient, low-wage countries such as India.[2] In 2004 over 80% of US companies considered outsourcing their information technology services to destinations such as India.[3] U.S. companies outsourced approximately $3 billion business processing work in 2005, reflecting a 65% increase from the previous year.[4] The business processing work included the transfer of personal data for processing insurance claims, credit card transactions, and transcription of personal medical files.[5] India's outsourcing and

---

[2] In April 2004 Unisys announced that it had set up a software development and back-office center in India. After its initial round of hiring 2,000 people by the end of 2005, its employee base in India would double in 2-3 years. Unisys also plans to invest $180 million, increasing over time. Unisys has acquired a state-of-the-art facility in the central business district in Bangalore, India, hired an experienced management team, and commenced operations. Governments and public sector institutions are among Unisys' largest customers. The company handles sensitive information such as police records and homeland security databases, some of which will move to India. Unisys wards off criticism that this could lead to a compromise on data security by claiming that it already out-sources work relating to sensitive data to some Indian firms and has had no problems with their performance. S. Srinivasin, *Unisys to Invest Heavily in India*, INFORMATION WEEK, April 28, 2004, *available at* http://networks.org/?src=infoweek:19202134 (last viewed May 25, 2004). *See also* UNISYS, *Unisys Chairman Anticipates Growth in India Resources*, *available at* http://www.unisys.co.in/about__unisys/news_a_events/03298525.htm (last viewed March 12, 2006).

[3] *See* National Association of Software and Service Opportunities, *"India: A 'Secure' Market for Outsourcing"* May 10, 2004, *available at* http://www.nasscom.org/artdisplay.asp?Art_id=2552 (last viewed November 18, 2004).

[4] India, China, the Philippines and Eastern Europe are among the countries taking on the bulk of this work. Aryn Baker, *In Search of the Next Bangalore*, TIME, 43, June 26, 2006. According to Gartner, Inc., a leading provider of research and analysis on the global information technology industry the vast majority of offshore business process outsourcing ("BPO") is around contact centers, including voice, e-mail and chat, and the remainder for processing services. *See* Gartner Press Release 2004, *available at* http://www.gartner.com/5_about/press_releases/asset_79327_11.jsp (last viewed December 1, 2005).

[5] As many as 500,000 U.S. tax returns containing confidential information regarding individuals and entities were projected to be prepared in India over the past two years. The predicted annual numbers are a significant and rapid increase from 25,000 tax returns in the 2002 tax year and 100,000 for 2003. The individual and business returns are being transferred to India for processing by not only sole-ownership CPA firms, but also by some of the largest accounting firms in the U.S. *See* Liz Pulliam Weston, *Your Financial Secrets Are Headed Overseas,* MSN MONEY, *available at* http://moneycentral.msn.com/content/Banking/FinancialPrivacy/P90682.asp?Printer (last viewed December 1, 2005). Similarly, TransUnion, one of the three major credit bureaus, plans to send all consumer disputes to a processing center in India. The company expects a significant increase in such disputes as U.S. consumers take advantage of a new law requiring bureaus to provide free annual credit reports, and says outsourcing the work is its most cost-effective option. Credit-bureau files contain highly sensitive financial data, including Social Security numbers, credit account numbers, the amounts owed and the payment history. David Lazarus, SAN FRANCISCO CHRONICLE, *Credit Agencies Sending Our Files*

electronic technology industry generated revenues of $36 billion in 2005, reflecting a 28% increase from 2004.[6]

As the wave of outsourcing swells, the issue of information piracy and data security in India has come under greater scrutiny. The absence of appropriate statutory measures in India is becoming increasingly of great concern to investors, corporations, the legislature and the public in other nations.[7] India is being urged to enact an adequate data protection regime which dictates the appropriate parameters for the collection, storage and use of personal data by private and government entities.[8] Given the international focus on India's date protection scheme, it is merely a matter of time before India enacts data protection laws. However, since intellectual property rights that lack enforcement are worthless, the seminal issue that remains once the data protection laws are in place is whether the laws will be enforced in such manner as to provide any meaningful protection to data.[9] The existing enforcement regime in India's legal system

---

Abroad, Nov. 11, 2003, *available at* http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2003/11/07/MNG4Q2SEAM1.DTL (last viewed December 1, 2005).

[6] See, *10 Ways India is Changing the World*, TIME, 41, June 26, 2006, *citing* World Bank, United Nations, McKinsey and Co., PriceWaterhouseCoopers Report, *Forbes* and Government of India.

[7] The United Kingdom's Labor party Members of European Parliament affiliated with the Amicus trade union in the U.K. announced in April that they would ask the European Union's executive branch, the European Commission, to protect British consumers whose personal data is being transferred to India, warning that offshore outsourcing is "an accident waiting to happen." John Ribeiro, *Indian Law May Satisfy EU Data Protection Concerns*, COMPUTERWORLD, April 21, 2004, *available at* http://www.computerworld.com/printthis/2004/0,4814,92557,00.html (last viewed December 12, 2005). *See also* Stuart Lauchlan, *The Blame Game*, THE AGE, May 3, 2005, *available at* http://www.theage.com.au/articles/2004/09/20/1095651229660.html?from=storyrhs (last viewed December 12, 2005); Steve Ranger, *Security Worries Hit Offshore Outsourcing*, SILICON.COM, April 26, 2005, *available at* http://management.silicon.com/itdirector/0,39024673,39129859,00.htm (last viewed December 12, 2005).

[8] *The International Legal Framework for Data Protection and its Transposition to Developing and Transitional Countries,* GLOBAL INTERNET POLICY INITIATIVE (December 28, 2004).

[9] *See* Robert M. Sherwood, *The TRIPS Agreement: Implications for Developing Countries*, 37 IDEA 491 (1997), *citing* Renato Ruggiero, Message from the Director-General of the World Trade Organization, in The Intellectual Property and International Trade Law Forum: Special Issue 1998 XV (1998) ("Laws for

is pitifully deficient, marred by interminable delays in moving matters through the existing court system. India will be unable to provide adequate protection to data unless a solution is found to address the court delays, and procedures established for expediently prosecuting data protection breaches and compensating those harmed.

The paper recommends a system of specialized courts that deal with data protection and other cyber infringement matters. After analyzing specialized courts in various other jurisdictions and assessing their viability in India, a proposal is made for specific features for a Cyber Infringement Court in India.

II. MODELS OF DATA PROTECTION AND PRIVACY LAWS

A. The Emergence of the Issue of Data Protection

The protection of data finds its roots in the individual's right to privacy doctrine.[10] The right to privacy has been explicitly contained in or has inferentially been found to exist in the constitutions of most developed nations and the jurisprudential parameters of privacy rights explored in various forums.[11] However, the specific privacy issue related

---

the protection of intellectual property rights are of no account if intellectual property rights cannot be effectively enforced."); Michael L. Doane, *TRIPs and International* I*ntellectual Property Protection in an Age of Advancing Technology*, 9 Am. U.J. Int'l L. & Pol'y 465, 482 (1994) (stating that "[i]ntellectual property rights are useless without adequate enforcement provisions."); Arthur Wineburg*, Jurisprudence in Asia: Enforcing Intellectual Property Rights*, 5 U. Balt. Intell. Prop. L.J. 25, 27 (1997) (stating that enforcement of intellectual property laws is intractable problem); Arthur Wineburg & Edmund H. Mantell, M*anaging Intellectual Property--An International Capital Asset*, 99 Com. L.J. 366, 368 (1994) ("The value of intellectual property depends upon the extent of one's rights to it are recognized and enforceable.").

[10] PETER CAREY, DATA PROTECTION, A PRACTICAL GUIDE TO UK AND EU LAW 1 (2d ed. 2004).

[11] The UK does not have a written constitution, and the right to privacy is not explicitly protected in the UK. In 1990 the Calcutt Committee, charged with conducting an inquiry into press behavior in regard of personal privacy, concluded that there was no satisfactory definition of privacy in the UK. However, the Committee concluded that the right to privacy could be legally defined as "[t]he right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information." *Report of the Committee on Privacy and Related Matters,* Cm. 1102, HMSO, 1990. A further attempt to define privacy came from the government of the UK in its Response to the National Heritage Select Committee, where it stated that "[e]very individual has a right to privacy comprising: (a) a right to be free from harassment and molestation; and (b) a right to privacy of personal

to protection of personal data became an issue of growing concern in progressive nations in the 1970s with the advent of computerized systems which could store and disseminate large amounts of information with relative ease via automated processes.[12] In the UK, the Younger Committee on Privacy was instituted in the early 1970s to make recommendations regarding the manipulation of computerized personal data.[13] Similarly, in the US the Data Privacy Act of 1974 was enacted.[14] Subsequent protection of the privacy of personal information was accomplished in the UK and US through various legislative enactments.[15] However, the gold standard for data protection was established by the European Union in 1995 with the passage of EU Directive 95/46/EC.[16] The Directive established comprehensive legislation for data protection, setting a high

---

information, communications, and documents." *Government Response to the National Heritage Select Committee, Privacy and Media Intrusion*, Cmnd. 2918, HMSO, 1995.

Although the US Constitution does not explicitly provide for a right to privacy, this right has been found implicit in provisions of the First, Fourth, Fifth, and Fourteenth Amendments. *See* Ryan Moshell, … *And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Towards Comprehensive Data Protection*, 37 Tex. Tech L. Rev. 357, 373 (Winter 2005). With regard to the collection of private information, specifically, the U.S. Supreme Court, in *Whalen v. Roe*, recognized the "… threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files." *Id*. at 373; *Whalen v. Roe*, 429 U.S. 589, 605 (1977). Similarly, the Constitution of India does not expressly recognize the right to privacy, although it does provide that "[n]o person shall be deprived of his life or personal liberty except according to procedure established by law." Constitution of India, Article 21, November 1949, *available at* http://www.alfa.nic.in/constt/a1.html (*last viewed* June 17, 2006). A mere 14 years after the inception of the Indian Constitution, the Indian Supreme Court recognized a right to privacy implicit in the Indian Constitution pursuant to Article 21. *Kharak Singh v. State of UP*, 1 SCR 332 (1964).

[12] Carey, *supra* note 11. Similarly, in the US the Privacy Act of 1974 was enacted to prevent the misuse of personal data. 5 U.S.C. § 552a.

[13] Carey, *supra* note 11, at 1-3.

[14] *Infra* note 33.

[15] The UK passed the Data Protection Act of 1984. *See* Carey, *supra* note 11, at 3. The US has enacted piecemeal legislation including the Fair Credit Reporting Act and the Privacy Act of 1974. *See infra* note 33.

[16] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, EU

standard for non-EU member states to meet. The EU's regime impacted non-EU member nations directly because under the Directive data could not be transferred to states which did not provide adequate standards for protection. The EU standard for data protection is briefly described below, and the impact of this legislation on other nations – the US and India – is examined in subsequent sections.

B. The European Standard

EU Directive 95/46/EC ("Directive") was adopted in October 1995 for the purpose of mandating standards within the then 15-member European community for the protection of personal data.[17] As with all EU directives, the Directive was not self-implementing. It required all EU member states to enact, no later than October 25, 1998, national legislation giving effect to its provisions to protect individual citizens' rights to privacy and to prevent the unauthorized dissemination of its citizens' personal information both within and outside the EU.[18]

Directive 95/46/EC, *available at* http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm (last visited August 6, 2006).

[17] *Id*. *See also*, Kevin Bloss, *Raising or Razing the e-Curtain?: the EU Directive on the Protection of Personal Data,* 9 Minn. J. Global Trade 645 (Summer 2000), *citing* W. Scott Blackmer et al., Online Consumer Data Privacy Regulation in the U.S., Elec. Banking L. & Com. Rep. Apr. 1999, at 1.

[18] Bloss, *supra* note 18, *citing* Henry J. Perritt, Jr. & Margaret G. Stewart, False Alarm?, 51 Fed. Comm. J.L. 811 (1999).

At present, all 25 members of the EU have enacted legislation giving effect to the provisions of the Directive. *See*, Directive, *supra* note 17; implementing data *available at* http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm (*last viewed* August 6, 2006). Should a problem with implementing the Directive have arisen, the European Commission would step in to resolve non-compliance by the EU Member State. The implementation of legislation in the EU is the primary role of the European Commission, an independent executive body consisting of 25 Commissioners (one from each EU Member State). The Commission, intended to be a body independent of Member States, is not permitted to take instructions from the government of any Sate. Maintaining such independence permits the Commission to represent the interests of the citizens of the EU in its role as the upholder of legislation and treaties. *See, generally*, EU Institutions and Other Bodies, *available at* http://europa.eu/institutions/index_en.htm (last viewed August 6, 2006).

The Directive proposes a broad-brush 'umbrella' legislation encompassing all sectors of industry and all instances of collection and use of personal data. The Directive protects " … the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data …."[19] The processing of data can be wholly or partially by automatic means.[20] Personal data encompasses information relating to an identified or identifiable natural person 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" (*emphasis added*).[21] "Processing of personal data" is defined as any operation performed upon personal data "… whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction … ."[22] In essence, all personal data held must comply with the following principles:

- Personal data must be processed fairly and lawfully, with discosure of the controller of the data, and disclosure of the purpose for which it is being collected;

- Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

[19] Directive, *supra* note 17, Chapter I, Article 1, 1.

[20] *Id.* at Chapter I, Article 3, 1.

[21] *Id.* at Chapter I, Article 2 (a).

[22] *Id.* at Chapter I, Article 2 (a).

- Personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

- Personal data must be accurate and, where necessary kept up to date. Reasonable steps must be taken to ensure that inaccurate, misleading or incomplete data is erased or rectified;

- Personal data must be kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which data were collected or for which they are further processed. Member States are required to establish appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific purposes. [23]

With regard to enforcement of the data protection laws, the Directive requires EU Member States to provide judicial remedies to any individual whose rights to data privacy are violated. It also requires that Member states adopt suitable measures to ensure the implementation of the Directive, and to impose sanctions on the data collectors and processors for violations of any section of the Directive.[24] Several EU Member states, including the UK and Italy have adopted specialized courts with exclusive jurisdiction over intellectual property matters.[25]

A critical aspect of the Directive is its impact on the global economy. Data transfer to third countries or regions outside the EU is permitted only if the recipient

[23] *Id.* at Chapter II, Section I, Article 6. *See also*, Carey, *supra* note 11, at 51-63.

[24] Directive, *supra* note 17, at Chapter III, Articles 22, 24.

[25] *See generally, infra* notes 131-156 and accompanying text.

nation provides an "adequate level of protection."[26] Pursuant to this case by case approach under Article 25 of the Directive, the adequacy of the level of protection afforded by a third country is assessed by the European Commission which is empowered to produce a list of countries which ensure an adequate level of protection by virtue of the third country's domestic laws or international commitments for the protection of private lives, basic freedoms and rights of individuals.[27] Factors such as the nature of the data, the purpose and duration of the processing operation, the country of origin, the country of final destination, the rules of law in place in the third country, the professional rules and security measures complied with in that country are considered in reaching an

---

[26] Any meaningful analysis of adequate protection must comprise the two basic elements: the content of the rules applicable, and the means for ensuring their effective application.

In the absence of a finding of adequacy, a data controller can still transfer personal data to such a country by using one of the eight alternative procedures, such as using an approved contract, or obtaining the consent of the data subject (the individual to whom the personal data relates). Transfer of personal data to the third country may proceed if (i) the data subject has given his or her unambiguous consent to the transfer; (ii) the transfer is necessary either for the performance of a contract to which the data subject is party, or the transfer is necessary for the implementation of pre-contractual measures taken in response to the data subject's request; (iii) the transfer is necessary to conclude a contract, or to perform a contract, between the data controller and someone other than the data subject, in cases where the contract is entered into at the request of the data subject, or where the contract is in the interests of the data subject; (iv) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; (v) the transfer is necessary to prevent the vital interests of the data subject, including injury or other damage to the data subject's health, or to prevent serious damage to his or her property; (vi) the personal data to be transferred are an extract from a statutory public register, i.e. a register established by law as being available for public consultation, or as being available for consultation by persons with a legitimate interest in its contents. Directive, *supra* note 17,Article 25(1), 26(1).

[27] *See*, Directive, *supra* note 17, at Article 25(6). One difficulty of this case by case approach is that many countries outside the EU do not have standardized, homogenous protection in all economic sectors. For instance, many countries have data protection laws in the public, but not in the private sector. In the United States the sectoral approach to legislation makes the situation especially difficult: for example, specific laws exist for specific areas such as credit reporting and health industry, but not in others. Countries which have federalist systems, including Canada and the US, add an extra dimension of difficulty since the various states that form the federation may have different laws. Whether the protection afforded to a data transfer was representative of the entire country or only of a particular sector or state is a question that must be addressed in such countries. Report of the EUROPEAN COMMISSION WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, Free Movement of Information and Data Protection, including international aspects, 1997, *available at* http://www.privacyexchange.org/tbdi/EUID/EUadeq.html (last viewed July 30, 2006).

"adequacy" determination.[28] The fear of a prohibition on transferring data to a third country, with far reaching economic and trade repercussions, has encouraged certain third countries to adopt data protection measures similar to those of the EU.[29] Adoption of such laws, it is hoped, will lead to a finding of adequacy by the European Commission, thereby preserving trade and economic relations of the third country with the EU. At present, the European Commission has concluded that the laws of Switzerland, Isle of Man, Canada, Argentina, the US and Guernsey provide adequate protection.[30]

Article 26(2) of the Directive provides an exemption to the "adequacy" finding, opening up the possibility of *ad hoc* solutions to find adequate protection for data. The foremost alternative avenue is the creation of contractual arrangements between parties to fill in the gaps to ensure adequacy. The EU Commission has approved "model contracts" to assist data controllers in this regard, and such contracts would automatically fall under this provision. The Data Protection Commissioner also has the power to endorse "model contracts" specific to the transferring countries' circumstances, as well as the power to approve particular contracts or other arrangements that provide satisfactory safeguards. [31]

---

[28] *See* Directive, *supra* note 17, at Article 25(2).

[29] Latvia, hopeful that it would attain EU membership, was quick to enact legislation on data protection which encompassed the mandate of the Directive. Switzerland and Norway have also promulgated Directive-compliant legislation. Ryan Moshell, *supra* note 12, at 388, 389.

[30] Data Protection- European Commission, Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries, *available at* http://europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_en.htm (last viewed December 11, 2005). In the case of Canada, the approval is qualified. While there are several data protection laws in Canada, the European Commission's decision relates only to those data regulated by the Canadian Personal Information Protection and Electronic Documents Act 2000. Carey, *supra* note 11 at 107. In the case of the US, the EU and the US have entered into a "safe harbor" arrangement, *See supra* notes 36-43 and accompanying text.

[31] Procedurally, however, the Directive deals with these Article 26 contractual cases very differently from Article 25 cases. Under Article 25 Member States are required to notify each other and the Commission in cases where adequate protection has *not* been ensured and the transfer has therefore been blocked. By

Non-EU states who have not been found adequate with regard to their data protection regime primarily rely on contractual arrangements to continue their business transactions with EU Member States.

The US has circumvented the processes established by the Directive, neither meeting the EU's adequacy standard, nor conducting commerce through contractual arrangements with EU Member States. The unique arrangement between the US and EU Member States, the "Safe Harbor" arrangement, is described below.

C. The US Compromise

As explained above, the Directive mandates and EU nations have adopted a comprehensive legislation approach which, for example, requires creation of government data protection agencies, registration of data bases with those agencies, and in some instances prior approval before personal data processing may begin. In contrast, the U.S. approach to data privacy is "sectoral," in that it relies on a mix of legislation, regulation, and self regulation. Starting with the Fair Credit Reporting Act - the first legislation at a Federal level in the US to regulate private sector use and disclosure of personal information - and later the Privacy Act of 1974 which was enacted due to concerns about breaches of privacy arising from computer databases, the US has a system of data

---

contrast, under Article 26 the obligation is reversed: Member States are required to inform the Commission and other Member States of each authorization granted. This legislative arrangement addresses the fear that contractual solutions have inherent problems, such as the difficulty of enforcement of contractual rights by a data subject. Directive, *supra* note 17, at Article 26(2). *See also,* Report of the EUROPEAN COMMISSION WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, Free Movement of Information and Data Protection, including international aspects, 1997, *available at* http://www.privacyexchange.org/tbdi/EUID/EUadeq.html (last viewed July 30, 2006).

protection that is governed sector by sector.[32] At a state level, numerous laws protect the privacy of individuals.[33]

The US was concerned that its "sectoral" approach to data protection, quite different from the EU's 'umbrella' approach, would not meet the EU's standards of "adequacy." Fearing a disruption of commerce between the US and EU Member States that would hurt both businesses and consumers, the US Department of Commerce entered into negotiations with the European Commission in 1997 in an attempt to resolve the looming trade disaster.[34] In the summer of 2000 the U.S. Department of Commerce and the European Commission unveiled a "Safe Harbor" framework designed to bridge the differences between the EU and U.S. approaches to privacy protection.[35] On July 27, 2000, the European Commission determined that the US Safe Harbor privacy principles provided adequate protection under Article 25(6) of the Directive.[36] The finding of

---

[32] The Fair Credit Reporting Act, enacted in 1970, has been amended in 2003 by the Fair and Accurate Credit Transactions Act. *See also*, The Privacy Act of 1974, 5 U.S.C. § 552a.

[33] For example, the privacy laws in California include California Penal Code Section 502 which relates to computer crimes, prohibiting the intentional access of any "… computer system or computer network from the purpose of devising or executing any scheme … to defraud or extort or obtain money, property or services with false or fraudulent intent, representations, or premises; or to maliciously access, alter, delete, damage, or destroy, any computer system, computer network, computer program or data;" California Elections Code Sections 2188 and 2194 regulate the confidentiality of information such as the residential address, telephone number, occupation contained in voter registration records; California Civil Code Section 1799.3 prohibits video stores from disclosing its customers' personal information, including sales and rental information; disclosure of medical records to third parties is prohibited without written consent of the patient under California Civil Code Section 56. *See* Beth Givens, Privacy Rights Clearinghouse, Privacy Laws of the State of California*, available at* http://www.privacyrights.org/ar/callaw.htm (*last viewed* April 4, 2006).

[34] Aaron Lukas, Safe *Harbor or Stormy Waters? Living With the EU Data Protection Directive*, CATO INSTITUTE, CENTER FOR TRADE POLICY STUDIES, Publication 16, October 30, 2001, at 2.

[35] *Id*.

[36] Article 25(6) of the Directive provides, in relevant part, that "[t]he Commission may find … that a third country ensures an adequate level of protection … by reason of its domestic law or of the international

adequacy is binding on the Member States of the EU, and permits US organizations which participate in Safe Harbor to be deemed adequate under the Directive. By eliminating the need for approval from the EU prior to data transfers, the process of transferring data to US Safe Harbor entities is streamlined, and continued flow of data to these US companies is assured.[37] Organizations formed in the US are eligible to participate in the Safe Harbor agreement.[38] Safe Harbor is essentially a self-regulatory approach whereby US entities which self-certify that they are compliant with the principles of Safe Harbor.[39] The Safe Harbor principles track the principles contained in the Directive, closing any loops that may exist between the US sectoral laws and the requirements of the Directive. The seven Safe Harbor Principles are:

---

commitments it has entered into … for the protection of the private lives and basic freedoms and rights of individuals." Directive, *supra* note 17, at Chapter IV, Article 25(6), *available at* http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm (*last viewed* December 21, 2005).

[37] US Department of Commerce, Safe Harbor, *available at* http://www.export.gov/safeharbor/sh_overview.html (*last viewed* August 6, 2006).

[38] *See* Jan Dhont, María Verónica Pérez Asinari, and Prof. Dr. Yves Poullet et al., *Safe Harbour Decision Implementation Study*, EUROPEAN COMMISSION, April 19, 2004, at 13, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/safe-harbour-2004_en.pdf (*last viewed* August 6, 2006), stating that an organization must be established in the US to be eligible for Safe Harbor. US subsidiaries formed in countries other than the US are ineligible. *See also* Commission Decision, Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbor Privacy Principles, *available at* http://www.export.gov/safeharbor/DecisionSECGEN-EN.htm (*last viewed* August 6, 2006).

[39] These self-certifying entities are listed on the US Department of Commerce website as organizations that EU Member States may transfer data to. US Department of Commerce, Safe Harbor, *supra* note 38. *See also*, EUROPA, European Commission, Justice and Home Affairs, *Freedom, Security and Justice*, *available at* http://europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/adequacy-faq1_en.htm (*last viewed* March 30, 2006). The self-certifying US entity is required to re-certify every year thereafter. *See* US Department of Commerce, Safe Harbor, *supra* note 38.

- Conspicuous *notice* must be provided to the data subject regarding the purpose of the data collection and use, as well as regarding complaint mechanisms available to the data subject;

- *Choice* must be offered to the data subject to opt out if the data is being used for a purpose that is different than its original purpose, or if data is to be transferred to third parties. The data subject is given an opt-in choice if the data is sensitive, relating to race, religion, ethnicity etc.;

- *Onward transfer* of personal data to third parties may only be done consistent with the principles of notice and choice;

- The data subject must be permitted *access* to his or her information collected by the US entity;

- The *security* of the personal data must be maintained by exercising reasonable precaution to ensure that data is protected from loss;

- The *integrity of data* must be maintained, ensuring that it is relevant to the purpose for which it was collected, accurate and current;

- The self-certifying US entity must provide mechanisms for *enforcement* of the Safe Harbor principles. Data subjects must be provided a forum for filing complaints, and a dispute resolution procedure established to respond to grievances of the consumer.[40]

[40] *Id*.

US organizations may incorporate the seven Safe Harbor principles in various ways. For instance, organizations may adopt safeguards deemed necessary by the EU for transfers of personal data from the EU to the US by incorporating the relevant safe harbor principles into agreements entered into with parties transferring personal data from the EU. In the alternative, where an organization is subject to US statutory, regulatory, administrative or other body of law (or body of rules issued by national securities exchanges, registered securities associations etc.) that also effectively protects personal data privacy, it qualifies for Safe Harbor to the extent that there is a nexus between its activities and the specific laws or rules.[41] With regard to enforcement of data privacy laws, given the US' sectoral approach, violations of data privacy in the US may be prosecuted by the Federal or state authorities in corresponding courts, or by the administrative agency under whose jurisdiction the sector is being regulated or legislated.[42] Although the US has adopted a number of specialized courts, at present none deals exclusively with data privacy matters.

---

[41] *Id.*

[42] For instance, in an administrative action brought by the Federal Trade Commission ("FTC"), an internet company that provides online shopping cart software to online merchants was charged with wrongful disclosure of personal information about its customers to marketers. The FTC entered into a settlement with the defendant, under the terms of which the defendant was barred from use of the personal data the company has already collected, as well as from making future misrepresentations about the collection, use, or disclosure of personally identifiable information. The settlement also required the company to ensure that consumers received a clear and conspicuous notice before their personal information was disclosed to other companies for marketing purposes. *In the Matter of Vision I Properties, LLC, doing business as CartManager International***,** File No. 042 3068, *available at* http://www.ftc.gov/opa/2005/03/cartmanager.htm (*last viewed* April 4, 2006). See also, *In the Matter of Sunbelt Lending Services, Inc.,* FTC File No.: 042 3153; *In the Matter of Nationwide Mortgage Group, Inc., and John D. Eubank,* FTC File No. 042-3104, Docket No. 931. *available at* http://www.ftc.gov/opa/2004/11/ns.htm (*last viewed* April 4, 2006), where the FTC brought administrative charges against two mortgage companies for violation of the Gramm-Leach-Bliley ("GLB") Safeguards Rule. The Safeguards Rule, which implements the security requirements of the GLB Act, requires financial institutions to have reasonable policies and procedures to ensure the security and confidentiality of customer information. The companies charged with the violation, Nationwide Mortgage Group, Inc. and Sunbelt Lending Services, Inc., were charged with not having reasonable protections for customers' sensitive personal and financial information.

Early analysis of the Safe Harbor arrangement indicates mixed success and of the Safe Harbor arrangement. While the number of self-certifying US entities has continued to grow, the enforcement mechanism provided by these companies has come under fire. Less than 50 companies had chosen to be placed on the Safe Harbor list a year after its inception.[43] This number had multiplied significantly four years later, with 842 companies self-certifying on the US Department of Commerce site's Safe Harbor list on December 15, 2005. Of these 842 self-certifying companies, 728 organizations had self-certified within the last twelve months that they were "current" with their certification status. 114 organizations had not certified or re-certified in the last year, or had notified the Department they no longer adhered to the safe harbor framework, and were identified as "not current" in their self-certification. Almost 14% of the companies self-certifying were not current in their compliance: organizations that are "not current" are not assured the benefits of Safe Harbor.[44] Should the number of companies failing to re-certify or which are not current with their compliance continue to increase, the success of Safe Harbor will be questionable.

A Safe Harbor Implementation Study conducted at the request of the European Commission acknowledged the increased participation by US companies in Safe Harbor and briefly noted a handful of other positive trends, while criticizing the Safe Harbor in length on numerous grounds.[45] The privacy policies of companies has been severely

---

[43] Aaron Lukas, *supra* note 35.

[44] US Dept. of Commerce, *Safe Harbor List*, *supra* note 38.

[45] In addition to noting the increased participation by US companies, the study also briefly acknowledged four additional positive trends related to the Safe Harbor. A considerable number of countries listed in the Safe Harbor list certified that they would cooperate with the European data protection authorities,

criticized due to their inaccessibility and lack of clarity. Companies' representations that they had instituted privacy programs were generally found to be dubious, unsupported, and inconsistent with the Safe Harbor privacy program definition. Finally, the reviewers were critical of the alternate dispute resolution mechanism adopted by US companies on the grounds of inadequacy, lack of procedural transparency and sanctioning regimes.[46]

Breaches in data security, such as that reported by Lexis-Nexis in March 2005 involving personal information of 32,000 US residents,[47] as well as by the shoe retailer DSW Inc. which reported that credit card numbers of people who shopped at 103 of its 175 stores had been obtained by hackers, have not helped build confidence in the US data protection regime. U.S. companies reported more than 60 data breaches between January and September 2005, and Congress, as well as a number of state legislatures, responded with dozens of pieces of legislation, many modeled after a 2003 California law requiring companies to notify affected customers about data breaches.[48] In November 2005 the

---

indicating a positive attitude. Some companies provided information in their privacy policies which was not strictly required by the Safe Harbor principles. US data processors generally affirmed the existence of security measures. Finally, the report noted that Safe Harbor adherents generally provided their full contact information on the Department of Commerce self-certification, while concurrently noting negatively that the privacy policies did not always contain adequate contact information). Jan Dhont et al., *Implementation Study*, supra note39, at 59.

[46] *Id*. at 62-77

[47] Fraud artists assumed the identities and used the passwords of legitimate customers to download customer data including names, addresses, driver license numbers and social security numbers. Jonathan Krim and Robert O'Harrow Jr., *Data Under Siege ID Thieves Breach LexisNexis, Obtain Information on 32,000,* WASHINGTON POST, March 10, 2005, *available at* http://www.washingtonpost.com/wp-dyn/articles/A19982-2005Mar9.html (last viewed December 22, 2005).

[48] California Civil Code Section 1798.29 was enacted in acknowledgment of the fact that the privacy and financial security of individuals was increasingly at risk due to the ever more widespread collection of personal information by both the private and public sector. At the Federal level, the far-reaching IDENTITY THEFT PROTECTION ACT was introduced in July 2005. S.1408, 109th Cong., 1st Sess. (2005). S.1408 would require entities to develop and maintain a scheme for the security of sensitive personal data collected or transferred by the entity. This legislation is yet to be enacted. Similarly, the FINANCIAL DATA PROTECTION ACT of 2005 was introduced in October 2005. H.R. 3997, 109th Cong., 2nd Sess. (2005). This

Senate Judiciary Committee was referred a bill that would require companies with data breaches to notify affected customers, and would set up rules for the U.S. government's use of private databases.[49] The bill would require businesses holding the personal data of more than 10,000 U.S. residents to conduct risk assessments and implement data-protection policies. Failure to implement security plans could expose businesses to fines up to $35,000 per day.[50] Despite the outcry over the dozens of breaches this year, Congress has been reluctant to pass a data breach notification bill, partly because of growing concerns that most of the bills would take a step backward from existing state laws.[51]

Whether packaged in one piece of legislation as the EU Directive is, or whether in a more piecemeal sectoral fashion, both the US and the EU have well-defined and comprehensive laws on data security and privacy. The EU members have adopted comprehensive data protection law covering all sectors. The US has sector-specific laws and laws at the federal and the state level. Despite the presence and strength of laws in the US and EU, breaches such as the Lexis-Nexis failure have occurred with regard to data transferred electronically. Comfort can be derived from the presumption that

---

bill, as yet to pass, would mandate a strong Federal standard whereby entities would be required to notify consumers of breaches involving potential identity theft.

[49] PERSONAL DATA PRIVACY AND SECURITY ACT of 2005, S.1789, 109th Cong., 1st Sess. (2005).

[50] *Id*.

[51] *See* remarks of Senator Leahy on May 25, 2006 that "[r]ather than work on our privacy and identity theft legislation, including the Specter-Leahy Personal Data Privacy and Security Act of 2005 … we are being directed to another divisive debate on a proposed constitutional amendment [to keep to a political timetable for raising divisive matters in the runup to the November elections]." 152 CONG. REC. S 5217 (2006). *See also*, Grant Gross, *Data Breach Bills Unlikely to Pass Before 2006, Frequency of Notifications One Sticking Point in Legislation*, PC WORLD, November 14, 2005, *available at* http://www.pcworld.com/news/article/0,aid,123515,00.asp (last viewed December 22, 2005).

enforcement of the laws in the US and the EU will serve to deter future criminals, and to offer recourse to the victims of data piracy. Although critical due to the infusion of IT business to India, as the remainder of this paper discusses, such comfort is available neither with regard to the data protection laws in force in India today, nor as to the enforcement of existing or prospective laws.

D. Current Data Protection Laws in India

India does not currently have a specific data protection law. Data protection and privacy are given scattered and rather sparse coverage by existing laws. The existing data protection laws, discussed in some detail below, are strewn in laws pertaining to information technology, intellectual property, crimes, and contractual relations. Under increasing pressure from BPO operations and call centers in India that handle large volumes of data from the US and Europe, the Indian government is contemplating the passage of a comprehensive law protecting data. Despite the urgency of the matter and pressure from internal and external fronts, India has delayed enactment of legislation for several years.[52] The form of the legislation - whether umbrella, sectoral or a combination of the two - which will provide optimal protection for cross-border data processed in India has been under discussion for several years. At this point, it appears likely that India's Information Technology Act of 2000 ("IT Act of 2000") will be amended to incorporate laws that provide comprehensive protection to data.[53] This approach, which

[52] An amendment to the IT Act of 2000, offering enhanced protection to data, was close to enactment in 2004, after 7 years in the making; unfortunately this proposed amendment was shelved due to a change of India's Central government. Andy McCue, *Offshore Data Protection Law Flounders*, SILICON.COM, *available at* http://www.silicon.com/research/specialreports/offshoring/0,3800003026,39130054,00.htm (*last viewed* December 12, 2005).

[53] THE INFORMATION TECHNOLOGY ACT, 2000, Order under Ministry of Law, Justice and Company Affairs (Legislative Department), June 9, 2000. The IT Act of 2000 covers cyber and related information technology laws in India. It deals essentially with authentication of electronic records and electronic

continues to be discussed as the probable solution to India's data protection dilemma, does not entail enactment of a separate comprehensive law to deal with data security and privacy issues across all industries, as has been the case with the EU.[54]

Until such time as India enacts adequate data protection laws, the current laws in India are the only protection offered for data privacy violations. These existing laws, including the IT Act of 2000 which is the most pertinent since it pertains specifically to the use of computer data, and their shortcomings are discussed below. It is observed that unlike the Directive which imposes liability on each participant within the chain of command of the data who failed to protect the sanctity of the data, India's existing laws only prosecute those individuals who directly violate laws related to computer systems or copyright.[55] Entities are exempt for breaches of data privacy unless such a violation was made knowingly.[56] Unlike the Directive which protects data breaches by limiting its collection and use, the Indian laws do not specify conditions under which data can be collected and used.[57] Where liability may be found by stretching the existing laws to

---

signatures, lacking specific provisions relating to privacy of data, data interception and computer forgery. Report of the Expert Committee, *Proposed Amendments to Information Technology Act 2000*, Department of Information Technology, Ministry of Communications & Information Technology, Government of India, August 2005, *available at* http://www.mit.gov.in/itact2000/Summary-final.doc (*last viewed* August 2, 2006). *See also*, Sufia Tippu, *Indian IT Act to be Amended to Net Cyber Criminals*, IT WIRE, July 13, 2006,
available at http://www.itwire.com.au/content/view/4957/945/ (*last viewed* August 2, 2006).

[54] Another alternative that was discussed, but is unlikely to be enacted, is an 'umbrella' data privacy law similar to the EU Directive, which allows for sectoral adjustments. This proposal would encompass the EU's comprehensive and expansive legislation, while retaining the flexibility of the US's sectoral approach. This proposal was offered by Rodney Ryder, a member of committee considering data privacy/protection laws in India. A copy of Mr. Ryder's March 1, 2006 email which addresses this issue is in the files of the author of this paper.

[55] *Infra* notes 60, 85 and accompanying text.

[56] *See infra* notes 61, 62, 85, 86 and accompanying text.

[57] The Directive mandates five principles in accordance with which data must be collected and processed, including the requirement that the collection of data must be specific to the purpose for which it is

cover breaches of data privacy, penalties afforded to victims are inadequate in a transnational context.[58] The existing Indian laws and their deficiencies are addressed in further detail below.

1. IT Act of 2000

The IT Act of 2000, Section 43(b) affords cursory safeguards against breaches in data protection.[59] The scope of Section 43 (b) is limited to the unauthorized downloading, copying or extraction of data from a computer system, essentially unauthorized access and theft of data from computer systems. Section 43(b) is limited in scope, and fails to meet the breadth and depth of protection that the EU Directive mandates. The law creates personal liability for illegal or unauthorized acts, while making little effort to ensure that internet service providers or network service providers, as well as entities handling data, be responsible for its safe distribution or processing. Furthermore, the liability of entities is diluted in Section 79 of the act, which inserts "knowledge" and "best efforts" qualifiers prior to assessing penalties.[60] A network service provider or intermediary is not liable for the breach of any third party data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.[61] Similarly, while Section 85 of the Act does invoke entity

---

collected, and such purpose must be disclosed to the data subject. *Supra* note 24 and accompanying text. See also, *generally, infra note 60* and accompanying text.

[58] *Infra* notes 65-69, 87 and accompanying text.

[59] IT Act of 2000, *supra* note 54, at Ch. IX Section 43(b).

[60] IT Act of 2000, *supra* note 54, at Ch. XII Section 79.

[61] *Id*.

liability, such liability is limited to the specified illegal acts under the IT Act of 2000 which does not offer broad protection of data.[62] Section 85 does extend liability to key employees (managers, directors, officers etc) of the company for intentional or negligent acts that result in a breach of the specific violations under the IT Act of 2000.[63]

With regard to damages available in the event of a breach of data privacy, Section 43(b) is deficient in that the maximum penalty for this breach is monetary compensation in the paltry amount of approximately two hundred and twenty thousand dollars ($220,000).[64] The maximum monetary damages available for a breach that can potentially be several times more, is clearly inadequate in a transnational context. The law makes no differentiation based on the intentionality of the unauthorized breach, and no criminal penalties are associated with a breach of Section 43(b). The more limited crimes of computer hacking and tampering are considered criminal offenses under the IT

---

[62] *Id*. at Ch. XIII Section 85. Section 85 (1) provides that

> (1) Where a person committing a contravention of *any of the provisions of this Act* (*emphasis added*) or of any rule, direction or order made thereunder is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:
>
> Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place *without his knowledge or that he exercised all due diligence* to prevent such contravention. *(Emphasis added).*

[63] *Id*. at Section 85 (2). Section 85 (2) provides that

> (2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the *consent or connivance of, or is attributable to any neglect* on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly. *(Emphasis added).*

Act of 2000: Section 65 offers protection against intentional or knowing destruction, alteration, or concealment of computer source code with. Section 66, while offering no clear language which protects personal data, offers limited protection when personal data is destroyed, deleted or altered. Both Sections 65 and 66 are punishable with criminal penalties including jail time of up to 3 years or a monetary penalty of up to $440,000.[65] In addition to Sections 65 and 66, although Chapter XI of the IT Act of 2000 specifies criminal penalties for a laundry list of illegal acts, no such recourse is available for the broad realm of breaches of personal data security.[66] In addition to the protections discussed above, Section 72 of the IT Act of 2000 offers some protection for breaches of confidentiality and privacy.[67] Non-consensual disclosure of confidential information is punishable by imprisonment for up to 2 years, or a maximum fine of approximately $220,000.[68]

---

[64] *Id.* at Section 43(b), 43(h).

[65] *Id.* at Sections 65, 66. Section 65 provides that "[w]hoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees [approximately $440,000], or with both."

Section 66(1) provides that "[w]hoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack." Section 66(2) provides for penalties similar to Section 65 (*see supra*).

[66] *Id.*, at Ch. XI.

[67] *Id.*, at Ch. XI, Section 72, Section 72 provides that "[s]ave as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book. register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both."

[68] *Id*.

In contrast to the IT Act of 2000, the EU Directive envisions much broader violations associated with breach of data security than does the limited sphere of the IT Act of 2000.[69] As described previously, the EU Directive provides for protections in the entire chain of control of data, and creates systems of security and associated penalties within the various stages of data processing.[70] For instance, the Directive prescribes limits to the collection of personal data, requiring that a purpose for the data collection be articulated.[71] The Directive also requires that data must be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject; personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.[72] The 1980 Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data promulgated by the Organization for Economic Cooperation and Development (OECD) are also instructive, demonstrating that a large void exists in India's IT Act of 2000. A reformation of the IT Act of 2000 should encompass the principles contained in the Directive, and the parallel OECD principles related to limitation of data collection, data quality, specified purpose, use limitation, security safeguards, individual participation and accountability.[73]

---

[69] *See supra* note 20 and accompanying text.

[70] *Supra* note 23 and accompanying text.

[71] *Supra* note 24, and accompanying text.

[72] *Id.*

[73] Principles of the Directive are discussed *supra* at note 24, and accompanying text. *See also*, Organization for Economic Cooperation and Development, Information Security and Privacy, Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data , *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (last viewed August 6, 2006). The OECD Guidelines were formulated in anticipation that member nations, including the US,

Further, in matters of trans-national data protection the IT Act of 2000 is deficient in that jurisdiction for cases arising out of violations lies in India. A special tribunal is established by the Central Government, and all matters arising out of the IT Act of 2000 are within the jurisdiction of this Cyber Appellate Tribunal.[74] While the IT Act of 2000 is diligent in establishing a tribunal headed by a qualified judicial officer, the difficulty in accessibility to this tribunal is stark in a trans-national setting. Injured parties who are non-residents of India would have to adjudicate disputes in a foreign jurisdiction, incurring the related expense ad inconvenience thereof. The limited parties from whom recourse can be sought, limited circumstances under which remedy may be established, and the limited nature of the damages is even more bare when the avenues for recourse and compensatory sums are viewed from a perspective of third party nationals.

2. Additional Sources of Legal Protection in India

In addition to the scattered provisions of the IT Act of 2000, the Indian criminal laws and intellectual property laws also afford limited protection for personal data. As illustrated below, these provisions contain many gaps making the overall existing data protection scheme in India inadequate. Given this sparse and scattered protection, the most prevalent mode of data protection is contractual arrangements between the data collector, the transferee and the data subject. These additional data protection regimens are addressed below.

---

had agreed to pass legislation pertaining to data protection and privacy. The Guidelines were meant to address the threat that disparities in national legislations could hamper the free flow of personal data across national borders. It was anticipated that the flow of data would greatly increase with the innovation and spread of computer and communications technology.

[74] IT Act of 2000, *supra* note 54, at Ch. IX, Section 46, 47, and Chapter X, Sections 48 et seq.

a. Indian Criminal Laws: The Indian criminal laws do not specifically address breaches of data privacy. Under the existing Indian Penal Code, liability for such breaches must be inferred from tangentially related crimes. For instance, Section 403 of the Indian Penal Code imposes criminal penalty for dishonest misappropriation or conversion of "movable property" for one's own use.[75] Movable property has been defined as property which is not attached to anything, and not land: although no jurisprudence has developed on this interpretation, arguably, movable property encompasses computer-relayed data and intellectual property.[76] Wrongful misappropriation of data, or conversion for one's own use may, under this interpretation, be punishable as a crime in India.

In addition, Indian Penal Code Section 405 provides criminal penalties for criminal breach of trust. Section 405 provides that "[w]hoever, being in any manner entrusted with property, or with any dominion over property, dishonestly misappropriates or converts to his own use that property, or dishonestly uses or disposes of that property in violation of any direction of law prescribing the mode in which such trust is to be discharged, or of any legal contract, express or implied, which he has made touching the discharge of such trust, or willfully suffers any other person so to do, commits "criminal breach of trust"." Liability under Section 405 extends to employees and agents of the violator, and the crime is punishable by imprisonment and/or fine.[77]

[75] INDIA PEN. CODE Section 403.

[76] INDIA PEN. CODE Section 22, defining "movable property" as "… corporeal property of every description, except land and things attached to the earth or permanently fastened to anything. which is attached to the earth."

[77] INDIA PEN. CODE Section 405 *et seq.*

Section 424 of the Indian Penal Code provides criminal liability for dishonest or fraudulent concealment or removal of property. Accomplice liability is also envisioned, with jail and fines imposed on the first party or accomplice.[78] Sections 420 of the Indian Penal Code may also offer some protection for failure to adequately protect data. Section 420 pertains to dishonest delivery of property to a third person.[79]

While it was likely not envisioned at the time of enactment that the criminal laws referenced above would be used to offer protection for misuse of data, given the importance of the data processing industry to the Indian economy and seriousness of the harm from breaches in data privacy, Indian courts may extend the protections offered by these criminal statutes. The adequacy of the remedies under India's criminal laws in a trans-national context remains questionable, as is the case with the remedies under the IT Act of 2000.[80] Similarly, jurisdictional issues remain problematic- the cost, delay and inconvenience associated with foreign nationals bringing actions in Indian courts offsets the availability of the recourse.[81]

---

[78] INDIA PEN. CODE Section 424 provides that "[w] hoever dishonestly or fraudulently conceals or removes any property of himself or any other person, or dishonestly or fraudulently assists in the concealment or removal thereof, or dishonestly releases any demand or claim to which he is entitled, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both."

[79] INDIA PEN. CODE Section 420 states that "[w] hoever cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine."

[80] *See supra* notes 65-69 and accompanying text..

[81] *Supra* note 75.

b. Intellectual Property Law Protection

Computer software (including computer programs, databases, computer files, preparatory design material and associated printed documentation, such as users' manuals) have copyright protection under Indian laws. Computer programs per se are not patentable, being patentable only in combination with hardware.[82] Thus in India, by past practice and under current laws, copyright is the preferred mode of protect for computer software.

A 1994 amendment of the Copyright Act of 1957 brought sectors such as satellite broadcasting, computer software and digital technology under Indian copyright protection. Protection of intellectual property rights in India was considerably strengthened in 1999. In addition to major legislation pertaining to patent and trademark laws, the Indian Copyright Act of 1957 was amended to make it fully compatible with the provisions of the TRIPS Agreement.[83] Known as the Copyright (Amendment) Act, 1999 ("Indian Copyright Act"), this Act came into force on January 15, 2000.

---

[82] India Patents (Amendment) Act, 2005, Section 3(k) excludes "mathematical methods, business methods or algorithms" from the scope of patentability. *See also*, Manisha Singh, *India's Patent law – is it TRIPs compliant?*, MANAGING INTELLECTUAL PROPERTY, *available at* http://www.managingip.com/?Page=17&ISS=17631&SID=524402 (last viewed August 6, 2006).

[83] The World Trade Organization (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs) is an international treaty which sets down minimum standards for most forms of intellectual property regulation within member countries of the WTO. Specifically, TRIPs deals with copyright and related rights (ie. rights of performers, producers of sound recordings and broadcasting organisations); geographical indications (including appellations of origin); industrial designs; integrated circuit layout-designs; patents (including the protection of new varieties of plants); trademarks; and undisclosed or confidential information, (including trade secrets and test data). TRIPs also specifies enforcement procedures, remedies, and dispute resolution procedures. The obligations under TRIPs apply equally to all member states, however developing countries are allowed a longer period in which to implement the applicable changes to their national laws. WORLD TRADE ORGANIZATION, *Agreement on Trade-Related Aspects of Intellectual Property Rights*, *available at* http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm (last viewed December 20, 2005). *See also,* Wikipedia, *Agreement on Trade-Related Aspects of Intellectual Property Rights, available at*

The Indian Copyright Act prescribes mandatory punishment for piracy of copyrighted matter commensurate with the gravity of the offense. Section 63B of the Indian Copyright Act provides that any person who knowingly makes use on a computer of an infringing copy of computer program shall be punishable for a minimum period of six months and a maximum of three years in prison.[84] Fines in the minimum amount of approximately $1250, up to a maximum of approximately $5,000 may be levied for copyright infringement of computer software. An enhanced penalty is available for second or subsequent convictions- imprisonment for a minimum term of one year, with a maximum of three years, and fines between $2,500 and $5,000.[85] As with penalties under the IT Act of 2000, these penalties are inadequate in a transnational context.[86]

In addition to the strengthening of copyright laws, a number of measures have been taken in the past few years to strengthen the enforcement of copyright laws in India. Such measures include education and building awareness of copyright issues in the public sector (through state government offices and central government ministries), as well a private business (including company stakeholders, enforcement agencies, professional users like the scientific and academic communities and members of the public). The government has initiated a number of seminars and workshops on copyright issues whose

---

http://en.wikipedia.org/wiki/Agreement_on_Trade-Related_Aspects_of_Intellectual_Property_Rights (last viewed December 20, 2005).

[84] India Copyright Act, 1957, Chapter XIII, Section 63A, 63B.

[85] *Id.* Actual knowledge of the infringement is a pre-requisite to a finding of criminal liability. The actual knowledge standard protects bona fide users of software; in the case of copyright there are quite a large number of works which are in the public domain that a person can use freely, and it is natural for many to presume that such works are outside the copyright regime. *See*, EMBASSY OF INDIA, Policy Statements, *Intellectual Property Rights in India*, *available at* http://www.indianembassy.org/policy/ipr/ipr_2000.htm (last viewed December 21, 2005).

[86] *Supra* notes 62-54 and accompanying text.

participants include law enforcement personnel as well as representatives of industry organizations. Enhanced and specialized programs have been established to give law enforcement officials training in copyright issues. Judicial officers have been selected and trained to deal with these intellectual property violations.[87]

c. Contractual Relations: Private contractual terms have been used as a means for filling the gap left by the IT Act of 2000 and other laws in India. Until a tighter data protection legal regime is in place, the US and other countries out-sourcing to India are relying upon contractual obligations to impose obligations for protecting and preserving data. There is growing recognition within the out-sourcing industry that contractual obligations do not provide the most efficient or effective recourse. In the event of a breach of the security of data, getting effective remedy under the contractual obligations is time consuming and often insufficient. Contractual recourse can be sought only against the contracting party in violation of the contracted terms; the actual wrong-doer may not be liable in damages or for criminal penalties. Having appropriate statutory protection with associated penalties, sanctions, damages and other remedies would likely act as a more appropriate deterrent against the breach of data privacy.[88]

---

[87] The Indian government claims that as a result of the numerous measures to protect copyright initiated by the Indian government, enforcement activity has significantly increased. As per the data relating to copyright offenses available with the National Crime Records Bureau, the number of copyright cases registered went up from 479 in 1997 to 802 in 1998. The number of persons arrested increased from 794 in 1997 to 980 in 1998. The value of seizures has gone up from $720,000 (approximately) to $1,870,000 in 1998. *See*, EMBASSY OF INDIA, Policy Statements, *Intellectual Property Rights in India*, *available at* http://www.indianembassy.org/policy/ipr/ipr_2000.htm (last viewed December 21, 2005). By contrast, the International Intellectual Property Alliance (IIPA), a private organization representing the U.S. copyright-based industries in bilateral and multilateral efforts to improve international protection of copyrighted materials, finds that in the over fifteen years that IIPA has been studying copyright issues in India, there have fewer than twenty convictions for copyright piracy. INTERNATIONAL INTELLECTUAL PROPERTY ALLIANCE, *2005 Special 301 Report*, *available at* http://www.iipa.com/rbc/2005/2005SPEC301INDIA.pdf (last viewed August 6, 2006).

[88] Even though the government has delayed the implementation of a legal framework for prosecution of data and privacy breaches, Indian BPO companies have implemented processes such as the BS7799

3. Reform of Indian Data Protection Regime

The Indian system of data protection can be best described as a web – many protections are offered through various sources and the web traps some violations, but gaps and holes remain through which others slide through. In order to address the inadequacies of the IT Act of 2000 and the miscellaneous laws providing protection to data, Indian businesses and the Indian government drafted amendments which would fill the void. Although passage of the amended law covering data protection was anticipated in 2004, due to a change in government in 2004 the proposed legislation was shelved by the new government.[89] Whether the IT Acts is amended, or alternative legislation enacted to protect the sanctity of transferred data, the new laws must offer effective enforcement in order to conform to the "adequacy" norms of the Directive and the Safe Harbor privacy principles of the US. After the new rules are in force, India will enter discussions with the EU to get it to recognize India as a country that offers an adequate level of protection for personal data.

Enactment of law that facially provides protection is but one step in the fight to maintain the sanctity of data. Even if satisfactory data protection laws are in place in India, the real question in assessing the adequacy of the law is whether it will be effective in deterring wrongful data piracy. Two issues are examined in this context: First, the

---

standard for information security management of the London-based British Standards Institution. Standards such as BS7799, and the ISO17799 standard for information security of the International Organization for Standardization (ISO), based in Geneva, restrict access to certain data, or limit the quantity of data to be made available to employees of BPO and call centers. Security measures include limitation of software made available to the processor's workstation, denial of internet access so that information cannot be relayed by this means (for example, credit card information cannot be emailed via the internet), as well as creation of paperless offices so that data cannot be copied out. John Ribeiro, *India Poised to Tighten Data Protection Law*, COMPUTERWEEKLY.COM, April 22, 2004, *available at* http://www.computerweekly.com/Article130076.htm (last viewed December 12, 2005).

[89] *See supra* note 53.

general issue whether punishment deters crime. If it is concluded that appropriate sanctions do prevent and deter crime, the second issue is whether wrongful appropriation of data will be prosecuted in India sufficiently so as to be a deterrent. If the Indian enforcement system is found inadequate, alternative enforcement processes must be established to prosecute violations of data privacy. A system of specialized courts instituted in India to prosecute cyber infringement cases, including data privacy violations, is essential for this purpose. These post-enactment are discussed in Section III, below.

III. POST-ENACTMENT ISSUES IN INDIA

India has some laws already in place, and is headed towards adoption of more comprehensive legislation to protect data. The existing and proposed legislation, India's IT Act of 2000, the copyright laws and contractual arrangements, each carry remedies of monetary sanctions and/or imprisonment. Once amendments strengthening the current data protection laws are enacted, it remains to be seen if these remedies provide adequate protection against violations of data protection. If the laws are adequate, satisfying the stringent EU standards, it is absolutely vital to prosecute the data protection crimes in an efficient and expedient manner so as to act as a deterrent against future commission of crime. These issues are considered in the next two sections of this paper. However, even before the questions regarding punitive measures are addressed, it is important to know whether the enquiry is an appropriate one. The initial question whether punishment, in fact, deters individuals from committing crime is studied below.

A. Is Punishment a Deterrent Against Wrongful Conduct?

The empirical study of the effects of deterrence on wrongful conduct is an area of ongoing inquiry and lively debate.[90] A study of punishment and deterrence conducted in 1973 by Issac Erhlich is highly influential in the field of criminology.[91] Analyzing data over a period of three decades, Erhlich concluded that crime varied inversely with the probability of imprisonment and the average time served.[92] The proposition that crime is a negative function of (1) certainty of punishment, (2) severity of punishment and (3) the speed of punishment is now a theory that has gained acceptance by criminal theorists. Frequency of crime tends to decrease as punitive responses to crime increase in these three contexts.[93] For the purpose of this paper which focuses on enforcement issues, the first and third factors, certainty of punishment and speed (or celerity) of punishment are of special significance, and are discussed below.[94] The proposed legislative changes in

---

[90] Although the bulk of the analysis is focused on the deterrence of crime, it can easily be analogized to, and parallel conclusions drawn in regard to non-criminal misconduct. *See*, Michael K. Block & Vernon E. Gerety, *Some Experimental Evidence on Differences Between Student and Prisoner Reactions to Monetary Penalties and Risk*, 24 J. Legal Stud. 123 (1995).

[91] *Does Punishment Deter?*, NATIONAL CENTER FOR POLICY ANALYSIS, August 17, 1998, *citing* Isaac Ehrlich, *Participation in Illegitimate Activities: An Economic Analysis*, JOURNAL OF POLITICAL ECONOMY 81, 1973, pp. 521-64, reprinted in William Landes and Gary S. Becker, eds., ESSAYS IN THE ECONOMICS OF CRIME AND PUNISHMENT (1974).

[92] *Id*.

[93] STEPHEN E. BROWN, FINN-AAGE ESBENSEN & GILBERT GEIS, CRIMINOLOGY, EXPLAINING CRIME AND ITS CONTEXT, 193 (5th ed. 2004).

[94] An additional factor which is addressed only briefly in this paper is the personal characteristics of the wrong-does, and his propensity to commit crimes. Stephen J. Schulhofer, *Harm and Punishment: A Critique of Emphasis on the Results of Conduct in the Criminal Law*, 122 U. Pa. L. Rev. 1497, 1545 (1974). *See also*, Rudolph J. Berger, *Economic and Historical Implications for Capital Punishment Deterrence*, 18 Notre Dame J.L. Ethics & Pub. Pol'y 437, 441 (2004).

India contemplate severe monetary and jail sentences.[95] In contemplation of this, the severity of the punishment factor is not addressed in this paper.

Of the three identified factors, the *certainty of punishment* is seen to be a much greater deterrent than the severity of punishment.[96] It is estimated that a fifty percent increase in the probability of incarceration prevents about twice as much violent crime as a fifty percent increase in the average term of imprisonment.[97]

For crimes involving data piracy, which are categorized as non-violent or property crimes, the certainty of punishment is a much greater deterrent as compared to violent and sexual crimes.[98] Should businesses' internal crime detection processes, law enforcement mechanisms and the judicial processes be efficient and diligent in prosecuting computer-related crimes, the likelihood that data piracy will be deterred is great.

The second important factor in data piracy deterrence is the *celerity* or *speed of punishment*. It has generally been theorized and accepted by contemporary criminologists that the more speedily that punishment follows the commission of crime,

---

[95] In India where the per capita income at current prices US $349, the average fines for copyright protection are approximately 14 times the per capita income. Monetary sanctions in India's IT Act of 2000 are similarly daunting, and the proposed changes are expected to be even more arduous. These fines impose a significant burden on an individual and would act as a strong deterrent. EMBASSY OF INDIA, Policy Statements, *Intellectual Property Rights in India*, *available at* http://www.indianembassy.org/policy/ipr/ipr_2000.htm, (*last viewed* August 6, 2006).

[96] *But see Id.* at 1550, noting that " … it seems *possible to conclude*, contrary to some of the previous statistical studies, that severity does have a significant deterrent effect (and one more important than that of certainty) for several of the crimes examined." (Emphasis added).

[97] *Does Punishment Deter?*, NATIONAL CENTER FOR POLICY ANALYSIS, August 17, 1998, *citing* Michael K. Block and Vernon E. Gerety, *Some Experimental Evidence on Differences between Student and Prisoner Reactions to Monetary Penalties and Risk,* JOURNAL OF LEGAL STUDIES 24, January 1995, 138**;** Albert J. Reiss Jr., and Jeffrey A. Roth, eds., *Understanding and Preventing Violence* (Washington, D.C.: National Academy of Sciences, 1993), p. 6

[98] *Id.*

the more useful it is. To prospective offenders who are deliberating the commission of a wrongful act, the prospect of a swiftly-imposed enforcement, and therefore imminent punishment, creates a psychological cause-effect connection between the contemplated criminal behavior and the resulting punishment. This cause-effect connection strengthens in direct proportion to the celerity or speed with which the effect follows the cause.[99] Therefore, the swifter the probability of punishment, the less likely a wrong-does will be to commit an act of data piracy.[100]

The certainly and speed of punishment are critical factors in determining the effectiveness of sanctions. The two factors can be seen to interlink and function together in evaluating deterrence. These findings are critical to the Indian data protection scheme since they provide impetus for reform of the insufficient, lethargic and slow Indian law enforcement and judicial processes. Since crime is unlikely to be deterred under the deficient Indian system described in sub-section B below, the Indian enforcement mechanism must be given a major overhaul. A system of specialized courts dedicated to cyber infringement matters would resolve the deficiencies of the Indian enforcement system.

---

[99] Rudolph J. Berger, *Economic and Historical Implications for Capital Punishment Deterrence*, 18 Notre Dame J.L. Ethics & Pub. Pol'y 437, 441 (2004), *citing* Cesare Beccaria, On Crimes and Punishments 55-59 (Henry Paolucci trans., The Bobbs-Merrill Company, Inc. 1963) (1764).

[100] Convincing as the above data related to certainty of punishment and celerity of punishment is, it is naïve to assume that all persons follow the same calculus in making choices about whether to commit or refrain from committing a crime. In recent years criminologists have identified numerous individual characteristics that may be related to deterrence. For example, whether an individual shows preference for impulsive behavior or present gratification, versus delayed gratification could determine whether he can be deterred from committing a crime. The impulsive person would be more inclined to commit a crime since he would reflect less on the consequences of his act and therefore be less affected by them. Similarly, a person who is stimulated by the thrill of taking risks would be more driven by the excitement of the commission of the crime and less deterred by sanctions; an anti-authoritarian would consider rules and associated sanctions a threat to his right to self-regulate and would likely be less deterred by them. *Id.* at 199.

B. Delays and Inconsistencies in the Indian Enforcement Scheme

Assuming that the existing and proposed legislation in India sufficiently addresses the severity of punishment factors by imposing harsh monetary sanctions and jail sentences for misconduct related to data privacy breach, the issue to be considered in the Indian context are (1) certainty of punishment and (2) speed of punishment.

The Indian enforcement and judicial systems are fraught with delays, inefficiency and lethargy in both civil and criminal actions.[101] The Indian civil justice system exhibits a general failure to accommodate the demands of a newly market-oriented society. Typified by inefficient court administration, judicial passivity to an extent that is inappropriate in an adversarial legal system, and protracted, often discontinuous, trials, typify the legal process in India.[102] Inefficiency in court administration denies timely access to legal dispositions. Excessive control by litigants places those seeking legal redress in an unequal position because respondents can abuse and delay the resolution procedures with impunity. Finally, the unavailability of alternatives to litigation clogs the system. Many cases awaiting judgment are no longer contentious, and long-awaited judgments are often difficult to enforce.[103]

A peek into the window of civil litigation presents a disheartening picture. Records of new filings are kept by hand.[104] Documents filed in court are frequently

---

[101] Hiram E. Chodosh, Stephen A. Mayo, A.M. Ahmadi & Abhishek M. Singhvi, *Indian Civil Justice System Reform: Limitation and Preservation of the Adversarial Process*, 30 N.Y.U. J. Int'l L. & Pol. 1, 3 (Fall-Winter 1997-1998).

[102] *Id*.

[103] *Id*.

[104] *Id.*

misplaced or lost.[105] Lawyers crowd the courtroom and wait for their cases to be called. Once a matter is called, resolution is frequently delayed due to innumerable adjournments resulting from witness unavailability, absence of a party, witness or lawyer, or document unavailability.[106] Recordation of court proceedings is done by a judge who summarizes testimony for a court reporter, thereby losing specificity, precision and detail.[107] A case will not likely appear before the same judge for the duration of its cycle: transfer of judges occurs are a more expedient pace than judicial resolution.[108]

Unfortunately, the criminal court system offers no better picture. In India's overburdened court system, it can take up to seven years to complete a criminal case.[109] The challenge posed by the Indian enforcement system is that the criminal system is burdened by corruption, inefficient court procedures, lack of training, and inordinate delays. The gigantic trans-national problem of copyright infringement in India is illustrative of the initiatives that can be promulgated, and the results that can be expected. Following a strengthening of copyright laws a decade ago, a number of measures were taken by the Indian government to strengthen the enforcement of the laws. Such measures included training of enforcement officers, judicial officers and business personnel to build awareness of copyright issues, and assist in the detection of copyright

[105] *Id.*

[106] *Id.*

[107] *Id.*

[108] *Id.*

[109] IIPA, Special Report, *supra* note 88.

violations, and enforcement of copyright laws.[110] The results of the initiatives has been mixed: the Indian government claims that as a result of the numerous measures to protect copyright initiated by the Indian government, enforcement activity has significantly increased. As per the data relating to copyright offenses available with the National Crime Records Bureau, the number of copyright cases registered went up from 479 in 1997 to 802 in 1998. The number of persons *arrested* increased from 794 in 1997 to 980 in 1998. The value of seizures has gone up from $720,000 (approximately) to $1,870,000 in 1998.[111] The International Intellectual Property Alliance (IIPA), a private organization representing the U.S. copyright-based industries in bilateral and multilateral efforts to improve international protection of copyrighted materials, finds that in the over fifteen years that IIPA has been studying copyright issues in India, there have been fewer than

---

[110] Presumably as a result of the numerous measures to protect copyright initiated by the Indian government, enforcement activity has significantly increased. As per the data relating to copyright offenses available with the National Crime Records Bureau, the number of copyright cases registered went up from 479 in 1997 to 802 in 1998. The number of persons arrested increased from 794 in 1997 to 980 in 1998. The value of seizures has gone up from $720,000 (approximately) to $1,870,000 in 1998. *See*, EMBASSY OF INDIA, Policy Statements, *supra* note 88.

The situation, presumably prior to the mid-1990s which saw an amendment to the Indian Copyright Act and enhanced enforcement mechanism, was described in the following dismal terms: "The Indian court system presents a challenge to copyright enforcement. The Indian High Courts address copyright infringement only after cases meet exhaustive administrative requirements. The most difficult problem, however, lies at the lower criminal judiciary level where copyright cases remain the lowest priority. India's criminal system is extremely slow and cumbersome, which delays the litigation process and becomes an expensive endeavor for producers, directors, and actors who seek immediate enforcement against copyright violators. Trial delays also increase because investigators are frequently transferred to remote locations for other projects, and once they are relocated, securing their presence for a given case is difficult. Due to these delays, the investigators' evidence for the case is often misplaced or unusable; this helps the defendant obtain a motion to postpone the hearing or trial and further delays the litigation process. The slow, burdensome criminal court system has been detrimental not only to the enforcement of copyright laws on the national front, but also internationally … ." Priti H. Doshi, *Copyright Problems in India Affecting Hollywood and "Bollywood,"* 26 Suffolk Transnat'l L. Rev. 295 (2003).

[111] *See*, EMBASSY OF INDIA, Policy Statements, *supra* note 88.

twenty *convictions* for copyright piracy. [112] Therefore, while the detection of copyright violations may have dramatically increased and the number of arrests may have gone up significantly, the number of convictions remain poor. This points once again to the bottleneck at the courts. The state of the judicial system, with its inherent delays remains an unresolved burden.

The above discussion presents a gloomy picture of the prospects of enforcement of data protection laws in India. Even if appropriate data protection laws are enacted, they will likely be inadequate until enforcement issues are addressed. Monetary and criminal sanctions contained in the laws can deter instances of crime if the enforcement system is certain and speedy.

Given the problems of the Indian judicial mechanism and the fears that it will be grossly inadequate to deal with the added burden of cyber breaches (including criminal and civil breaches of data privacy), alternate means of enforcement must be envisioned and incorporated into the system of data protection in India.

C. Alternatives to Current Enforcement Regime in India

Once the data protection laws in India are strengthened, the general legal system must be tweaked to address data protection enforcement. Proposed remedies to fix the enforcement void include establishment of a national centralized enforcement body dedicated to, and trained in electronic data piracy and enforcement. This national body must be given jurisdictional authority to enforce across state borders. In addition, it is essential to have specialized local police enforcement units which are specifically trained and maintained to recognize instances of and enforce actions against data piracy crimes.

---

[112] *See*, IIPA, Special Report, *supra* note 88.

Finally, it is vital to adopt meaningful court reform to decrease burdens, costs and delays and ensure that cases are concluded promptly with deterrent penalties and damages.

Specialized judicial avenues of enforcement are the logical transition that India must make due to the inability of the regular court system in India to deal with the additional volume of cases that cross-border crimes will generate. The solution is the establishment of specialized cyber infringement courts with jurisdiction over all violations related to intellectual property, including data privacy (hereinafter referred to as "Cyber Infringement Courts").[113] The specific model for such a court depends on factors such as local customs and practices (including local procedural considerations),

---

[113] International tribunals dealing with cyber infringement are a second alternative. Given the cross border nature of cyber breaches, and the ever increasing global interactions pertaining to intellectual property (including data privacy), these international tribunals may be an appropriate and effective solution in the future. In addition to the more commonly recognized areas of intellectual property (patents, trademarks, copyright, trade secret and unfair competition), data protection, database protection and privacy rights are areas related to, and encompassed within a broad definition of intellectual property. Cyber infringement courts may logically encompass all or a subset of these areas of intellectual property. *See, generally*, INTERNATIONAL BAR ASSOCIATION, INTELLECTUAL PROPERTY AND ENTERTAINMENT LAW COMMITTEE, INTERNATIONAL SURVEY OF SPECIALIZED INTELLECTUAL PROPERTY COURTS AND TRIBUNALS (September 2005), p. 6, *available at* http://www.comml-iba.org/attachment/articles/88/Final_International_IP_Survey_15-09-05.pdf (*last viewed* April 9, 2006). This model may draw from the Council of Europe's Convention on Cybercrime, an instrument for international co-operation which was signed on November 23, 2001 by 26 Council of Europe member States and the four non-member States which had helped with the drafting (Canada, Japan, South Africa and the United States). The Convention requires parties to criminalize certain conduct that is committed through, against, or related to computer systems. Such substantive crimes include offenses against the confidentiality, integrity and availability of computer data and systems, as well as using computer systems to engage in conduct that would be criminal if committed outside the cyber-realm, i.e., forgery, fraud, child pornography, and certain copyright-related offenses. The Convention also requires parties to have the ability to investigate computer-related crime effectively and to obtain electronic evidence in all types of criminal investigations and proceedings. By providing for broad international cooperation in the form of extradition and mutual legal assistance, the Cybercrime Convention is intended to remove or minimize legal obstacles to inter-national cooperation that delay or endanger a State's investigations and prosecutions of computer-related crime. *See, The Convention on Cybercrime, a unique instrument for international co-operation,* COUNCIL OF EUROPE, November 23, 2001, *available at* http://www.coe.int/NewsSearch/Default.asp?p=nwz&id=802&lmLangue=1 (last viewed April 9, 2006). However, even at just a procedural level such international governance and enforcement would necessitate, among other things, that participating States (1) enter into a treaty subjecting themselves to the jurisdiction of the international cyber crime tribunal, and (2) create a common set of rules or laws, including enforcement procedures, that would govern the area of intellectual property. Given the time consuming and costly nature of this solution, burdened with conceptual and procedural hurdles, this potential response is not a viable solution in the immediate future, and is not addressed in this paper.

cyber infringement caseloads, number of judges, and monetary considerations.[114] Specialized courts established in Thailand, the US, and for a limited purpose Italy, are studied below with special attention to these factors. Several specialized Cyber Infringement Courts of both civil and criminal jurisdiction with features drawn from those established in Thailand, the US and Italy, are the necessary solution to India's overburdened system. Suggested features for this specialized Cyber Infringement Court system are recommended in Section IIIB(3)(ii) below.

1. What Are Specialized Courts?

Specialized courts are courts of limited, explicitly focused subject matter jurisdiction. This jurisdictional feature means not only that the backlog in the regular courts gets reduced, but also that cases that fall within the jurisdiction of specialized courts get heard in an expedient, efficient manner. Another important feature of specialized courts is that, in contrast to judges of general jurisdiction courts who hear cases that span the entire spectrum of law, judicial officers who serve on specialized courts are typically experts in that field of law.[115]

Specialized courts can offer advantages related to time and efficiency in several ways. *First*, such courts foster judicial efficiency by virtue of the fact that since experts are appointed to the bench in these courts, not much effort is expended in developing expertise to adjudicate the matters brought before them. This has the natural result of expediency in the processing of cases. The *second* advantage, a corollary to the first, is

---

115 IBA, International Survey, *supra* note 114, at p. 2.

[115] CENTRAL EUROPEAN AND EURASIAN LAW INITIATIVE, LEGISLATIVE ASSISTANCE AND RESEARCH PROGRAM, SPECIALIZED COURTS: A CONCEPT PAPER (June 25, 1996), p. 1, *available at* http://www.abanet.org/ceeli/publications/conceptpapers/speccourts/spc1.html (*last viewed* April 9, 2006).

that lawyers appearing in specialized courts expend less effort, and ultimately less client resources, in laying the foundational aspects of these complex areas of the law. In courts of general jurisdiction attorneys typically develop the legal framework by providing extensive background material through submissions to the court, in the form of written briefs etc., to ensure that the judge has access to as much information as possible to adjudicate the case appropriately.[116] Since judges in specialized courts are experts in the field and do not need this education, this directly results in focused submissions, resulting in time and cost efficiency to the attorneys and their clients. A *third* advantage of specialized courts is the uniformity in decision making and consistency in the application of the law. The expertise of the specialized court judges results in thoughtful, predictable and uniform rulings well grounded in the law, leading to certainty of decisions and containment of potential grounds for filing lawsuits. Therefore, courts are less likely to be burdened and overcrowded as fewer prospective litigants find grounds for bringing a dispute to court.[117] A *fourth* related advantage is that given the soundness of the judgments of the court of initial jurisdiction (the specialized court), appeals are less likely to be filed. Therefore, the burden on appellate courts is also likely to be significantly reduced. *Fifth,* efficiency of time and procedure is also a likely result of the specialized nature of the proceedings. Judges who are experts in the field can better assess the time, procedure and substance required to move a case forward. Improved case management techniques, include establishing pretrial deadlines, the discovery process, ruling on

[116] *Id.* at p. 12,referring to generalist judges as "novices at everything and experts at nothing."

[117] The uniformity of decisions and predictability in the case law can also be a cause for inefficiency. Counsel may determine that their chance of success in the specialized court is low due to the case law developed in these courts; a strategic decision may be made to posture the case in such a way that it falls within the jurisdiction of a general court. The effect of this is an unnecessary overburdening of the general court system, and an under-utilization of the specialized courts. See *id*. p. 14.

dispositive motions, moderating settlement proceedings, scheduling and conducting trials, etc. would result from the specialized judge who is familiar with the issues presented and would more effectively control the flow of litigation than a generalist judge. *Finally,* specialized courts can be used to support the generalized courts. Due to the fluctuating and often erratic nature of court filings and proceedings, it is conceivable that a specialized court may have a small caseload at times. In such instances, specialized courts can lend a helping hand to overburdened courts of general jurisdiction.[118]

Due to the numerous advantages offered by specialized courts they are a feature of the judicial systems of many countries, although their structure and function may vary. The first question to be addressed is the feasibility of specialized courts in India. This complex and involved question is merely touched upon in this paper in Section IIIB(2) below, since it would necessitate a comprehensive feasibility study beyond the scope of this article.

If specialized courts are a viable solution to the Indian enforcement dilemma, then the next question is what model of specialized Cyber Infringement Courts would best fit India's needs. The specialized intellectual property courts of Thailand, Italy and a selection of the numerous specialized courts of the US are generally reviewed in Section IIIB(3)(ii) below with a view to proposing specific features of a specialized Cyber

---

[118] *Id.* pp. 10-14. *But see*, *id*. pp 14-16 regarding a discussion on some of the disadvantages of specialized courts. One criticism stems from the fact that due to the expense associated with establishing these courts, specialized courts may be geographically placed at further apart than courts of general jurisdiction. Litigants would have to bear the burden and cost of travel to these scattered specialized courts, creating barriers to justice.

Infringement Court system with jurisdiction over civil and criminal intellectual property matters in India.

2. Are Specialized Courts a Feasible Solution to India's Problem of Enforcement of Data Protection?

Specialized courts pose special problems for developing countries such as India. A major hurdle, and in fact the greatest barrier, is the expense factor associated with establishment of and maintenance of these courts. These costs are not only a one-time cost, but are also recurring in nature. The establishment expenses include consultation expenses related to policy research and drafting and design of new legislation, training of judicial officers, court and enforcement staff, administrative costs, costs of acquiring and furnishing buildings to situate the specialized courts. Recurrent and ongoing costs must be reflected in a larger budget allocation for agencies enforcing the legislation, ongoing training of court and administrative personnel, and hiring and retention of specialized judges, court and administrative agency staff.[119]

While the inherent expense of establishing specialized courts is significant, India is one of the developing nations that can afford, and indeed, must afford the support of its computer industry. India's gross domestic product was 8.4% in 2005, topping $800 billion. It has grown at the second fastest rate in the world over the past three years, an average of 8%.[120] India's projected continued high economic growth, fueled in large part by the growth in the computer-related industry, is the incentive for investing in a

---

[119] IBA, International Survey, supra note 114, at p. 7.

[120] *See*, Alex Perry, *Bombay's Boom*, TIME, 41, June 26, 2006. *See also*, *10 Ways India is Changing the World*, TIME, 41, June 26, 2006, *citing* World Bank, United Nations, McKinsey and Co., PriceWaterhouseCoopers Report, *Forbes* and Government of India.

specialized court system that addresses breaches to the industry that is instrumental to India's incredible economic success. In other words, India cannot afford to 'bite the hand that feeds it.' If India is to meet economists' projections and develop into one of the largest economy in the world within the next three decades, it is essential that it " … must expedite socio-economic reforms and take steps for overcoming institutional and infrastructure bottlenecks inherent in the system."[121] The question, then, is not whether India can afford to establish specialized courts to address its enforcement problems. The appropriate question is whether India can afford to *not* invest in the security of its computer industry. If prompt enforcement is essential to deter crime, and if India's current judicial system is already overburdened, lethargic and inadequate, then the answer is clear. India must invest in a system of specialized courts to promptly and adequately adjudicate data privacy violations.

3. If Specialized Courts Can Help Resolve India's Judicial Backlog, What Are the Appropriate Features Of This Alternate System?

Crafting an appropriate model for a specialized cyber infringement court in India requires some understanding of the current court structure in India. The features of India's judicial structure are set forth in sub-section (i) below. Next, specific features

[121] Manoj Pant, *Start of a new era for India?,* THE ECONOMIC TIMES, April 7, 2006, *available at* http://economictimes.indiatimes.com/articleshow/1480585.cms (*last viewed* April 9, 2006).
At a meeting of finance ministers from Asia and Europe, global economic output was predicted to expand to an astounding rate of 4.5 percent. This growth is " … driven to a significant extent by rapidly developing economies such as … India, where growth is three or four times faster than in industrialised countries." Brian Love and Jan Strupczewski, *Ministers predict hot world economic growth in 2006,* REUTERS UK, April 9, 2006 , *available at* http://today.reuters.co.uk/news/newsArticle.aspx?type=businessNews&storyID=2006-04-09T153341Z_01_L08773825_RTRUKOC_0_UK-ECONOMY-EU.xml (*last viewed* April 9, 2006). *See also*, *India Economy Overview*, ECONOMYWATCH.COM, *available at* http://economywatch.com/indianeconomy/indian-economy-overview.html (*last viewed* April 9, 2006).

from the courts of Thailand, Italy and the US are analyzed in subsection ii, and finally proposed features for specialized courts in India are discussed in subsection (iii) below.

i. Indian Judicial System

The Indian Judiciary, along with the Legislative and Executive branches, are the three institutions of state governance in India.[122] Similar to the US Constitution, the Indian Constitution has conferred upon the Indian Judicial branch the power of review of legislative and executive action. Enforcement of fundamental rights guaranteed by the India Constitution has been entrusted to the Indian judiciary. The Indian Constitution provides for a single integrated system of courts to administer both federal (or Union) laws, and State laws. Three years after attaining independence from British rule, in January 1950 the Supreme Court of India was inaugurated. The Supreme Court is at the apex of the judicial system.[123] Its powers include broad original and appellate jurisdiction. The President, in consultation with the Prime Minister, appoints Justices of the Court. At the state level, a hierarchal step below the Supreme Court, are the High Courts, one each located in each State in India. The justices of the High Court are appointed by the President in consultation with the Chief Justice of the Supreme Court

[122] India is a constitutional democracy, comprised of twenty eight states, six Union Territories, and the Territory of Delhi (capital of India). It has a parliamentary system styled in the fashion of the British system. Its bicameral legislature consists of the upper house, or the Rajya Sabha, and the lower house, the Lok Sabha. Legislative power rests primarily with the Lok Sabha. The Prime Minister is the effective executive, though there is also a President who has limited powers. India's structure is explicitly federal, but with features that emphasize the power of the center over subnational units. The twenty eight states, as well as Delhi and the Union Territory of Pondicherry have elected (unicameral) legislatures; the Chief Minister of each state is the chief executive. Each state also has a Governor, although appointed by the President, the Governor of each state works under the guidance and direction of the Prime Minister.

[123] India has approximately 10,000 courts: 1 Supreme Court, 18 High Courts, 3,150 District Level Courts, 4,816 Munsif/Magistrate Courts and 1,964 Magistrate II and equivalent courts. BIBEK DEBROY, GOVERNANCE, DECENTRALIZATION AND REFORM IN CHINA, INDIA AND RUSSIA 344 (edited by Jean-Jacques Dethier,Boston, Dordrecht, London: Kluwer Academic Publishers, 2000), *available at* http://www1.worldbank.org/wbiep/decentralization/saslib/Chap12%20Debroy.pdf (*last viewed* March 25, 2006).

and the state's Governor. Similar to the situation at the Union (or Central) level, the State's Chief Minister can influence the Governor's advice. State High Courts also have both original and appellate jurisdiction, and they oversee the work of all courts within the State. Each State is divided into judicial districts, presided over by District/Sessions Judge. This is the court of original jurisdiction for civil and criminal matters. Below this court are lesser courts in each State that hear civil and criminal matters.[124]

Inclusion of a specialized Cyber Infringement Court system within the existing court structure could be accomplished in India if the system is flexible and adaptable to change. India has a history of accommodating changes to its legal system. Prior to the British occupancy, India had a localized "panchayat" system of resolving disputes.[125] Panchayats, typically constituted of five respected village elders, dealt with each issue of contention within the local community as a discrete matter. Social, cultural and religious considerations played a dominant role in the decisions of the elders. This localized and informal system of dispensing justice was far removed from the institutional courts established by the British.

India adapted well to the system of centralized courts and the tradition of common law introduced by the British. Since gaining independence from the British, India has retained the centralized court system introduced by the British, but has also recently reverted back to a form of the "panchayat" system. Lok Adalats- literally translated to

---

[124] Pawan Chaudhary 'Manmauji,' *Indian Judicial System, Its Nature & Structure and Distinctions Between Law and Justice*, in INDIAN JUDICIAL SYSTEM, NEED AND DIRECTIONS OF REFORM, 25-27 (S.P. Verma ed., Kanishka Publishers New Delhi) (2004).

[125] S.N MATHUR, NYAYA PANCHAYATS AS INSTRUMENTS OF JUSTICE, 25-27 (Concept Publishing Company New Delhi) (1997).

mean "people's courts," have now been established to encourage alternate modes of dispute resolution.[126]

In addition, India has moved a mere step away from specialized courts. Special tribunals have now become a feature of the Indian judicial system: the Central Administrative Tribunal, State Administrative Tribunal, Income Tax Appellate Tribunals, Family Courts and Labor Courts have also been established to ease court delays.[127] Under the present form of the IT Act of 2000 certain cyber crime cases (including unauthorized access to computers, unauthorized downloading of copyrighted data, and launching virus attacks) are to be decided by adjudicating officers appointed by the Central government. The adjudicating officer is required to be either a judge of the Indian High Court, or be a member of the Indian Legal Service for a minimum period of three years. The IT Act of 2000 also mandates that the adjudicating officers are to have exclusive jurisdiction, to the express exclusion of civil courts, for matters which an adjudicating officer is empowered by the IT Act of 2000 to determine. Appeals from such cases are to be heard by the Presiding officer of the Cyber Regulations Appellate Tribunal ("Cyber Tribunals") that is constituted under the IT Act of 2000.[128]

---

[126] *Over 300,000 Cases Pending in Supreme Court*, NEWKERALA.COM, February 27, 2006, *available at* http://www.newkerala.com/news2.php?action=fullnews&id=17210 (*last viewed* April 9, 2006). *See also infra* note 59.

[127] *Id.*

[128] THE INFORMATION TECHNOLOGY ACT, 2000, Section 46 et seq. *See also* Y.K. SINGH, CYBER CRIME AND LAW 235 (Shree Publishers and Distributors) (2005). Unfortunately, establishment of the Cyber Tribunal languished, and for a period of two years after the passage of the IT Act on October 2000, the Indian government had not yet exercised its powers of establishing the Cyber Tribunal, nor appointed the adjudicating officers. Ultimately, students of the Asian School of Cyber Laws filed a Public Interest Litigation in the Bombay High Court to compel the government to establish the Cyber Tribunals. The petitioners contended that they wrote letters almost a year ago to the Indian Ministry of Information Technology and the Ministry of Law, asking them to rectify this defect. Apparently no action was taken by these ministries, forcing the petitioners to file suit in the Indian High Court. Ruling for the petitioners, on

~~October 9, 2002 the High Court chastised the government for the undue delay, and directed it to expedite~~ the process of setting up of these enforcement agencies. Following this, the Central Government of India directed that the IT Secretaries of each state and Union territory should be appointed as adjudicating officers. See, A*djudicating Officers for Cyber Crimes Appointed in India,* ASIAN SCHOOL OF CYBER LAWS, *available a*t http://www.asianlaws.org/cyberlaw/archives/10_02_adj.htm (*last viewed* April 10, 2006). *See also* Rajneesh De and Stanley Glancy, *IT Act Languishes Thanks to Government Negligence*, EXPRESS COMPUTER, August 26, 2002, *available at* http://www.expresscomputeronline.com/20020826/cover.shtml (*last viewed* April 10, 2006).

Given (1) the adaptability of Indians to accommodate change to their legal system, evidenced by India's history; (2) the absolute necessity of finding alternatives to India's overburdened and inefficient courts; (3) the need to serve and support India's technology industry (which is instrumental in strengthening India's economy and is predicted to move India into one of the foremost economic powers in the world) by instituting appropriate enforcement mechanism that deal with violations; (4) the strength of India's economy and its ability to support the industry that is causing the economic upturn; and (5) the numerous advantages that specialized courts would offer not only in terms of data protection, but also in avoiding any further burdening of the existing court system, specialized Cyber Infringement Courts must be adopted in India. The specialized courts of Thailand, and the US, and to a limited extent the courts in Italy, are instructive to India with regard to the issues of jurisdiction, court composition and procedural issues.

ii. Features of Thailand, US, and Italy's Specialized Courts

Specialized courts in Thailand and the US are valuable models for India: Thailand is a developing economy, much like India. Its experience with the expense and infrastructural changes associated with establishment of specialized courts is especially instructive. The US experience with specialized courts is important to the discussion since it has a long history of such courts handling a variety of matters such as probate, tax and family relations. The courts in the US are constituted in various ways, and the experience gained from institutions in the US that have already gone beyond the experimental stage is especially valuable. With regard to these two nations, Thailand and the US, particular attention is given to a study of jurisdiction of the specialized court, composition or constitution of the court, and procedural features that enhance the

efficiency of the courts. The Italian specialized court is instructive for limited purposes: the multi-dimensional roles the judges undertake, and the variety of subject matters handled by these courts sheds light on the possible variant roles of specialized courts.

(a) Specialized Intellectual Property Courts in Thailand

Although Thailand recognized the importance of intellectual property rights as a necessity of trade and commerce with other nations, enforcement of the intellectual property rights remained a problem until promulgation of legislation in 1996, the Act for the Establishment of and Procedure for the Intellectual Property and International Trade Court ("IPIT Act").[129] In 1997 Thailand established and inaugurated the Intellectual Property and International Trade Court ("IPIT Court") authorized by the IPIT Act.[130] A separate and specialized court of original jurisdiction, the goal of the IPIT Court is to provide enhanced intellectual property enforcement. The IPIT Court employs specially trained judges, its own rules and procedures to expedite the processing of cases (such as hearings without adjournments), and equitable remedies such as preliminary injunctions.[131]

[129] Act for the Establishment of and Procedure for the Intellectual Property and International Trade Court B.E. 2539 (1996) ("IPIT Act"), passed by the National Assembly and promulgated in the Government Gazette on 25 October 1996, available at http://www.skandiproperty.com/Act for the Establishment of and Procedure.pdf (*last viewed* August 2, 2006). Under the IPIT Act, a Royal Decree was issued to inaugurate the Central Intellectual Property and International Trade Court on 1 December 1997.

[130] *Id*. *See also*, Andrea Morgan, *TRIPS to Thailand: the Act For the Establishment of and Procedure for Intellectual Property and International Trade Court*, 23 Fordham Int'l L.J. 795, 800, 824 (March 2000).

[131] IPIT Act, *supra* note 130, at Sec. 19, 27, 30; *see also* Rules 12-19 of the Rules for IPIT Cases.

The IPIT Act does not limit the IPIT Court's *jurisdiction* to only intellectual property and international trade cases.[132] In fact, with regard to criminal matters, where a single act gives rise to several offenses, such extended jurisdiction is mandatory; where several related offenses are filed as a single charge, the IPIT Court's jurisdiction is discretionary as to those offenses which would not ordinarily fall to it.[133]

With regard to the *composition* of the court, a panel of three specially trained judges of the IPIT Court is established for the purpose of hearing cases assigned to them.[134] Two of the judges are 'career' judges, and one is an "associate judge." [135] Career judges are required to have *competence* in the intellectual property – and international trade – areas of the law.[136] Associate judges are *experts* in the fields of intellectual property (and international trade).[137] Associate judges are often attorneys who specialize in these fields; they are appointed for a term of five years.[138] In order to gain additional expertise in the field, the IPIT Court is authorized to delegate the

---

[132] IPIT Act, *supra* note 130, at Sec. 7.

[133] *Id*., Sec. 35, 36. Section 35 provides that "[i]n a criminal charge where a single act violates several offences and one of offences falls within the jurisdiction of the intellectual property and international trade court, the court *shall* also accept other offences for adjudication." (Emphasis added). *Id.* Section 36 states that [i]n a criminal case where several related offences are filed in the same charge, and some of the offences are not within the jurisdiction of the intellectual property and international trade court, the court *may* accept all offences for adjudication or reject any one or more of the offences which falls outside its jurisdiction so that the prosecutor may file a new charge with the competent court. In reaching its decision, the court shall regard convenience and fairness as its prime consideration." (Emphasis added). *Id.*

[134] *Id*., Sec. 19.

[135] Morgan, *supra* note 131.

[136] *Id*.

[137] IPIT Act, *supra* note 130, at Sec. 15.

[138] *Id*.

examination of evidence to the officers of another court. In addition, the IPIT Court has the authority to call on any knowledgeable person or expert.[139]

Two procedural features of Thailand's IPIT Courts are notable: first, the power vested in the IPIT Court to promulgate its own rules of court, and second, the expeditious processing of cases. As to the first procedural aspect, the Chief Justice of the IPIT Court is empowered by the Act to formulate and issue the Rules of Court for the IPIT Courts.[140] These include procedural and evidentiary rules.[141] Where the Rules of the Court are silent, the Civil Procedural Code and the Criminal Procedural Code of Thailand provide the default rules. Granting the Chief Justice this power means that the Court can adopt new rules, or change rules as and when necessary, without undue delay. Inherent in this innovative system is that there is great sensitivity in the procedure of the Court due to which the Court can evolve and respond in an appropriate and timely manner.[142]

The second procedural feature of Thailand's IPIT Courts attempts to remove unnecessary delay and provide expedition remedies to the litigants. The Act mandates that hearings proceed without adjournment.[143] It also requires that the IPIT Court render

---

[139] IPIT Act, *supra* note 130, at Section 31. *See also* Morgan, *supra* note 131, at 800, 827-28 (March 2000), *stating*, in part, that "[p]rior to the establishment of the IPIT Court, intellectual property cases were heard by non-specialized judges, which often resulted in misapplications of the law and, moreover, misunderstandings of basic intellectual property concepts."

[140] IPIT Act, *supra* note 130, at Sec. 30.

[141] *Id*. The only limit on this power is that the rules cannot infringe on the rights of a defendant in a criminal case.

[142] *See*, Morgan, *supra* note 131, at 829-30.

[143] IPIT Act, *supra* note 130, at Sec 27. An exception is created in case of "unavoidable necessity." *Id*.

written judgment promptly.[144] This IPIT Court procedure starkly contrasts with the standard practice of Thailand's civil courts which hear each case for only one day per month.[145]

Further, in the interest of expedience in resolution, appeals to the decisions of the IPIT Courts may be made directly to the Supreme Court of Thailand.[146] To ensure that the Supreme Court of Thailand has the expertise necessary to rule on these appeals, the Act dictates that the Supreme Court establish a specialized division to hear IPIT Court appeals.[147]

(b) Specialized Courts in the US

The US has an extensive range of Federal and state specialized courts. Tax, bankruptcy, probate and family courts are but a few of such specialized courts. Some courts in the US share *concurrent jurisdiction* with other specialized or generalized courts. For example, Probate Courts, one of the models of specialized courts in the US, share concurrent jurisdiction with both specialized family courts as well as with general courts in the US. In other words, matters which fall within the jurisdiction of probate courts in the US may also fall within the subject matter jurisdiction of family or general courts. General courts are concurrently responsible for supervision of decedents' estates, conservatorships, guardianships of minors and incompetence of persons; family courts in the US are concurrently responsible for removal and termination of parents and

---

[144] *Id*.

[145] *See,* Morgan *supra* note 131, at 830.

[146] IPIT Act, *supra* note 130, at Sec. 38.

[147] *Id*. Sec 43.

guardians, and custody issues.[148] This system permits a general court to hear certain specialized matters, and vice versa. It is questionable whether such concurrent jurisdiction is desirable, and whether it may not be more efficient and concrete for the litigants if such issues are within the exclusive jurisdiction of the probate court. On the other hand, it may be more frustrating and time consuming for the litigant where certain matters related to a case are heard by one court, other matters related to the same case transferred to a specialized court.

The numerous Federal, state and administrative specialized courts are *constituted* in different ways. Typically, a single judge (versus a panel of judges as in the case of Thailand and Italy) hears cases in the US. The tax courts are used for illustrative purposes in this paper. Tax law is a particularly complex area of the law. Creation of the specialized Tax Court in the US mitigated the burden on the general courts to adjudicate issues in this specialized field. The Tax Court is comprised of nineteen judges, each appointed for a fifteen-year term of office. Ten other special trial judges are attached to a system that is parallel to the "small claims" court system- jurisdiction lies in the special trial judge where the amount in controversy is less than a certain sum of money. Trials are conducted by a single judge or by a commissioner appointed by the chief judge.[149]

Appointing judges to a limited term (a term of fifteen years in the context of the US Tax Court) is advisable if the area of law is unlikely to be a permanent fixture in the

---

[148] CENTRAL EUROPEAN AND EURASIAN LAW INITIATIVE, LEGISLATIVE ASSISTANCE AND RESEARCH PROGRAM, SPECIALIZED COURTS: A CONCEPT PAPER (June 25, 1996) ("CEELI"), Section VII.B.1, *available at* http://www.abanet.org/ceeli/publications/conceptpapers/speccourts/spc1.html (*last viewed* April 9, 2006).

[149] *Id*. at Section II.

legal landscape. If the number of cases in that area of the law is subject either to fluctuation such that it may remain dormant for long periods of time, or may disappear over time, it is wise to appoint judges for a limited term.[150] With regard to *procedural matters*, the US model of a "fast track" court system adopted by certain jurisdictions is an important and innovative feature in terms of court efficiency. California adopted the Trial Court Delay Reduction Act to ensure the timely disposition of civil and criminal cases in its court systems. The statute provides for judicial supervision of litigation, ensuring through an oversight and sanction process that cases progress through the system without undue delay.[151]

(b) Specialized Intellectual Property Courts in Italy

After years of debate, in June 1993 Italy adopted a system of specialized courts with exclusive jurisdiction over intellectual property matters.[152] Twelve specialized courts are established in specific cities and establish the territorial limit of each division's jurisdiction. These specialized courts are a special section of the Italian Court of Appeal.[153] Each division of the specialized court consists of a panel of at least six judges who have specific intellectual property skills. Each case is heard and decided by a panel

---

[150] *Id*. at Section I.E.4.

[151] CAL. GOV'T CODE § 68600 et seq. recommended that the Judicial Council of California adopt rules effective July 1, 1991, to be used by all delay reduction courts. The guiding principle was that litigation should require only that amount of time reasonably necessary for pleadings, discovery and preparation, and that any additional elapsed time constitutes delay which should be eliminated. In part, the rules established a case differentiation classification system based on the relative complexity of cases- longer periods being granted for the timely disposition of more complex cases.

[152] Margherita Bari, IP-Centric Courts Equal a Welcomed Change in Italy, *available at* http://www.mwe.com/index.cfm/fuseaction/publications.nldetail/object_id/2df80680-9b4b-488b-8d84-cee97b391f66.cfm (*last viewed* April 5, 2006).

[153] *Id*.

of three judges. Each branch of the specialized court is headed by a "president."[154] Provided it will not cause any delay in the handling of intellectual property cases, the judges assigned to the specialized division are required to deal with subjects other than intellectual property issues.[155] This particular feature is attractive in that overburdened courts of general jurisdiction are well served if the specialized courts handles some of their caseload in times when the specialized court is able to do so.

India's specialized Cyber Infringement Courts should draw from the experiences of the courts established in Thailand, the US and Italy. Some of the more desirable jurisdictional, compositional and procedural features of these systems are recommended below in the Indian context.

iii. Proposed Features of India's Cyber Infringement Courts

While specific characteristics of the Cyber Infringements Courts are critical to their success in India, equally important is the public's ability to access justice through these courts. India's specialized Cyber Infringement Courts would ideally be located in strategic locations so as to provide reasonable access to litigants. Given India's jurisdictional structure where there is one Supreme Court at the apex and a High Court in each State, at the very least one specialized court must be located in each State, and several others in each State strategically placed in proportion to the population density and anticipated flow of cyber infringement cases.[156] Although the expense associated with the creation of such a network of specialized courts may appear

---

[154] *Id.*

[155] *Id.*

[156] *See supra* note 125 and accompanying text.

prohibitive, India's economic outlook, and specifically the growth of the technology industry not only supports this judicial system to, but indeed mandates it.[157] Specific features related to the jurisdiction, constitution and procedures of the specialized Cyber Infringement Courts are identified below.

Jurisdiction of India's specialized Cyber Infringement Courts: Two subject-matter jurisdictional questions need to be addressed in instituting a specialized court: (1) whether jurisdiction of a specialized court should be limited to a only those cases that clearly fall within the specialized area of law, or whether it should be more inclusive to include related cases, and (2) whether the court should be a court of general subject-matter jurisdiction during times when its case load so permits. Both questions are answered in the affirmative in the Indian context.

With regard to the *first* "related issue" question, as has been the experience with Thailand specialized intellectual property courts, the specialized court may be faced with a situation where either (a) subject areas related to intellectual property - such as data privacy- are sought by claimants to be settled in the specialized court, (b) a single act gives rise to several offenses, only one of which is in the jurisdiction of specialized court, or (c) several offenses arise from related acts, including one under the exclusive jurisdiction of the specialized court.[158] In such instance the Indian specialized Cyber Infringement Court should have the power to extend its jurisdiction and exercise it over all the offenses. This flexibility would offer the benefit of certainty, as well as expedient

---

[157] *Supra* notes 120-122 and accompanying text.

[158] S*upra* note 134 and accompanying text.

resolution of the matters, all under one roof. The judge assigned to the specialized cyber infringement case would be familiar with the matter, and would be efficient in its disposition. If the related matter required it, the specialized cyber infringement court should have the flexibility, power and resources to retain an advisor. The advisor could be another jurist assigned temporarily to the specialized cyber infringement court. In the alternative and in the interest of time, an independent consultant could be retained – similar to what has been provided for in Thailand's IPIT Courts.[159]

The advantages of this jurisdictional solution in India are numerous. The already over-burdened general courts in India would have some of the case load taken off them entirely by the specialized court. The litigant would be served well in terms of time and cost since removal from one court to another is procedurally complicated and inherently time consuming. Further, the judge hearing the specialized matter would already be familiar with the case, and is in the best position to adjudicate it in its entirety. Where specialized consultation is necessary, the specialized judge would make that judgment call efficiently and resolve the issue in the best manner possible.

A related concern of jurisdictional consideration is one of concurrent jurisdiction. Contrary to the experience of US specialized courts, concurrent jurisdiction issues should be planned for and addressed in a manner that draws cases away from the general courts, and in to the Cyber Infringement Courts.[160] A concurrent jurisdiction problem is certainly conceivable within the broad category of cyber infringement or intellectual

[159] *See supra* note 140 and accompanying text.

[160] *See supra* note 1490 and accompanying text. US Probate courts offer an example of concurrent jurisdiction, which offer the benefit to litigants of time efficiency by having all matters heard by one court, even if that matter does not fall specifically within the specialization of the court.

property cases, especially if the specialized court accepts "related" matters, as prescribed above. It is foreseeable that the related matter which would ordinarily fall within the jurisdiction of the generalized court, is now heard by the specialized court as a "related" matters. A concurrent jurisdiction problem, where the specialized court took away related matters that may have ordinarily fallen within the generalized court's jurisdiction, would not be entirely undesirable in the Indian context for two reasons: first, the already over-loaded general jurisdiction courts would benefit from having matters taken away from them; second, specialist judges would be well served to have continuing exposure to matters outside their field of specialization.

The *second* subject matter jurisdiction issue pertains to the optimum use of specialized courts. In the interest of reducing the load on the already over-extended courts of general jurisdiction, India's specialized courts should take on matters of purely general subject matter in lax times or when the court docket permits it, as does the Italian specialized court.[161] This "cross-pollination" would also address, to some extent, the concern that specialist judges may adopt an elitist attitude and see themselves as hierarchically superior to the generalist judge.[162]

Composition of the Indian Court: The Indian specialized Cyber Infringement Courts must determine three issues vital to the constitution of its courts: (1) the qualifications of the judges appointed to its specialized courts; (2) the number of judges designated to each matter, and (3) the term of appointment of each judge. The first and second questions are inter-related to a degree; if the Indian specialized courts retain

[161] Supra note 156 and accompanying text.

judges with expertise in intellectual property issues, one judge should be assigned to each case. However, if expert judges are not retained, then perhaps a panel of judges with mixed levels of competence should be assigned to each case.

In answering the *first* question, provided that India has a sufficient number of experts who can serve on the judiciary, it seems that Thailand's model of combining "competent" career judges with "expert" associate judges demonstrates an inefficient system for India.[163] India has been a leader in technology issues, and should have no dearth of such expertise. It should not be difficult for India to constitute its specialized courts with a judiciary that has proficiency in intellectual property. In the event that a particular issue is beyond the expertise of the specialized judge, the specialized courts should have the authority to bring in an advisor to inform on this specific issue.[164]

Should the recommendation be followed and expert judges be retained in the Cyber Infringement Courts, then the answer to the *second* question regarding the number of judges assigned to each case, follows logically. While meeting the goal of infusing its overburdened system with additional judges to lessen the burden on the courts, India must remain conscious of the expense associated with establishing specialized courts and hiring competent judges to staff them. Assigning each matter to a panel of judges (as is the case with Thailand's IPIT Courts and the Italian specialized courts), versus one judge

---

[162] CEELI, supra note 149, at pp. 18, 19.

[163] *Supra* notes 135-139 and accompanying text.

[164] *See supra* note 140 and accompanying text.

would mean incurring the cost of hiring a larger number of judges to staff each case.[165] If the Cyber Infringement Courts judiciary is comprised of experts, one such specialist judge is well equipped to hear each case. This is essentially the model followed by the specialized courts in the USA.[166]

The *third* issue India needs to address in terms of constitution of its courts is the term of office to be held by each judge. Appointing judges to a limited term (a term of fifteen years in the context of the US Tax Court; a term of five years in Thailand's IPIT courts) is advisable if the area of law is unlikely to be a permanent fixture in the legal landscape.[167] If the number of cases in that area of the law is subject either to fluctuation such that it may remain dormant for long periods of time, or may disappear over time, it is wise to appoint judges for a limited term.[168] The field of intellectual property, although subject to constant change and evolution, is unlikely to disappear or fluctuate to any significant extent. However, if this is a factor in establishing lifetime tenure for judges, it can be addressed in India anticipating and permitting flexibility in the placement of these specialized judges. Specialized judges in India can be appointed with an explicit understanding that they may be re-located to other courts, including general

[165] Both Thailand and Italy's specialized intellectual property courts have a panel of three judges assigned to each case. *See supra* note 135 and accompanying text pertaining to Thailand's IPIT courts. In Italy, each division of the specialized court consists of a panel of at least six judges who have specific intellectual property skills. Each case is heard and decided by a panel of three judges. *Supra* note 155 and accompanying text.

[166] *Supra* note 150, and accompanying text.

[167] *See supra* note 151 and accompanying text describing the term of appointment of US Tax courts. *See also supra* note 139 describing that Thailand's associate judges appointed to its IPIT Courts are retained for a term of 5 years.

[168] *See supra* note 151, *citing* CEELI, *supra* note 149 at Section I.E.4.

courts. Given the historic trend of an ever-increasing burden on the general courts in India, it is certain that the re-location of the specialized judge to a general court would be welcome relief to the backlogged general courts.

To summarize the issue of constitution of the courts, since India's overburdened system requires the infusion of additional and new judges to lessen the burden on the court system, yet must maintain relatively low costs in doing so, India should: (a) hire career judges with expertise in intellectual property matters (as opposed to Thailand's system of expert associate judges, and competent career judges), (b) assign one career judge to each case brought before the specialized cyber infringement court (versus Thailand's model of a panel of three, consisting of two career and one associate judge, and Italy's model of a panel of three judges), (c) offer lifetime tenure for the specialized judge, to avoid the expense related to having judges rotate through the system, (d) following Thailand's example, delegate the examination of evidence to the officers of another court, provided that their dockets permit such delegation, and (e) retain any knowledgeable person or expert to gain further insight into the particular intellectual property issue (as does Thailand). [169]

Court Procedures: Two specific features related to court procedures are recommended for India's Cyber Infringement Courts: (1) rules of court specific to the specialized courts, and (2) an expedited process for resolution of cases.

Thailand's example is helpful to address the *first* issue. In Thailand, the Chief Justice of its specialized IPIT court can promulgate the rules of court. This power means

[169] *Supra* notes 164-169 and accompanying text.

that the Court can adopt new rules, or change rules as and when necessary, without undue delay. Inherent in this innovative system is that there is greater responsiveness in the procedure of the Court due to which the Court can evolve in a responsive fashion.[170] This feature is exceptionally significant in the Indian context, where bureaucratic delays frustrate the process.[171] India's specialized Cyber Infringement Courts must be allowed to evolve with their needs, and this power to adopt new rules or make changes to existing ones must lie with the court. However, rather than place all power in the hands of one individual, a panel of judges of the specialized court in India can be selected as court administrators to formulate and then approve such new or additional procedures.

Expediency in resolution of the cases is one of the main reasons specialized courts have been recommended for India in this paper. The US model of a "fast track" court system, and to some extent Thailand's model for expedient resolution of intellectual property matters instruct this *second* procedural issue.[172] California's Trial Court Delay Reduction Act to ensure the timely disposition of civil and criminal cases in its court systems, which provides for judicial supervision of litigation, ensuring through an oversight and sanction process that cases progress through the system without undue delay, is an important feature for India to adopt.[173] Thailand's IPIT Courts attempts to remove unnecessary delay and provide expedition remedies to the litigants by requiring

---

[170] *Supra* note 143 and accompanying text.

[171] *See supra* notes 42 and 129 for illustrations of the inefficiency in the Indian bureaucratic process.

[172] *See supra* note 152 describing California's "fast track" system of administering cases in order to monitor, guide and expedite their progress through the legal system. *See also supra* notes 144, 145 describing IPIT Court procedures designed to expeditiously handle cases.

[173] *See supra* note 152.

that hearings proceed without adjournment, and that once the matter is adjudicated the IPIT Court render written judgment promptly.[174] These features from the California and Thai systems are not only desirable for India, but indeed absolutely essential. This system is not entirely new to India since India has, in fact, adopted a fast track system in its general courts.[175] The specialized Cyber Infringement Courts must adopt an expedited process, requiring not only a general rule that cases be resolve expeditiously, but specific provisions for such timely and efficient processing of cases.

Another aspect of expedient resolution of matters is establishment of a procedure of direct appeals. In Thailand, in the interest of expedience, appeals to the decisions of the IPIT Courts may be made directly to the Supreme Court of Thailand.[176] To ensure that the Supreme Court of Thailand has the expertise necessary to rule on these appeals, the Act dictates that the Supreme Court establish a specialized division to hear IPIT Court appeals.[177] Given the backlog at the Indian Supreme Court it may appear at first blush to be questionable whether Thailand's example of referring cases directly to the Supreme Court would serve much benefit in the Indian context. However, when one factors in the bottleneck at the appellate court level in India, it is seen as imperative for cases involving data protection (and generally intellectual property cases) have direct access to the ultimate judicial authority, the Indian Supreme Court. In order to ensure

[174] *See supra* note 1445, 145.

[175] *Nod to 20 fast track courts, 4 Lok Adalats,* THE TRIBUNE, March 14, 2005, *available at* http://www.tribuneindia.com/2005/20050314/delhi.htm (*last viewed* April 23, 2006); see also V. Venkatesan, *For Fast Track Justice*, FRONTLINE, Volume 18, Issue 14, July 7, 2001, *available at* http://www.hinduonnet.com/fline/fl1814/18140910.htm (*last viewed* April 23, 2006).

[176] *Supra* note 147.

[177] S*upra* note 148.

expertise in the Supreme Court, a specialized division within the Supreme Court can be established to hear appeals from the specialized court, as with Thailand's IPIT Courts.[178] Should it not be feasible for the Indian Supreme Court to have this specialized division for intellectual property matters, India's Supreme Court should be empowered to retain experts to advise the Court, if necessary, once again as exemplified by Thailand.[179]

Expedient resolution envisions special procedures that provide shortcuts to the present dysfunctional and inefficient court system in India. Should specialized courts be adopted, they must absorb the successful features of other systems. The recommendations listed above draw extensively from the Thai system which exemplifies the application of specialized courts in a developing nation such as India, and the US system in which specialized courts have not only withstood the test of time, but have also been adopted in various permutations across varied areas of the law. This cross-sectional critical examination of the various specialized courts in the Thai and US jurisdictions offers India an opportunity to adopt an appropriate legal system to effectively enforce data protection laws and resolve its looming data protection crisis.

IV. CONCLUSION

Data protection is an issue that is gaining increasing importance as our trans-national exchange of private information grows. While the EU has adopted stringent legislation to protect data, and the US has reached agreement with the EU to offer protection, the Indian laws remain unsatisfactory. It is anticipated that India will soon enact legislation which will provide acceptable protection to private data. The issue that

[178] *Supra* note 147 and accompanying text.
[179] *Supra* note 140.

remains to be dealt with in the Indian context is, unfortunately, far larger than the enactment of strong protectionist laws. Laws act as a deterrent to wrongful conduct if they are applied with certainty and speed: both sadly deficient in the Indian judicial system. Unless addressed, the systemic problems of enforcement in India, and specifically of unresolved cases due to court delays, will continue to render India's data protection laws inadequate.

Cyber Infringement Courts, specialized courts with jurisdiction over all intellectual property and data protection issues, are a necessary solution to India's enforcement problems. India must expediently adopt this system of specialized courts in order to render adequate protection to data, and maintain its growing presence in the global technology arena.