VOLUME 4

IJLT | The INDIAN JOURNAL of LAW and TECHNOLOGY

2008

# IJLT | The INDIAN JOURNAL of LAW and TECHNOLOGY

ISSN 0973-0362

Volume 4
2008

SPECIAL COMMENT



ARTICLES



BOOK REVIEW



national law school of india university
bangalore

IJLT The INDIAN JOURNAL of LAW and TECHNOLOGY

VOLUME 4 2008



**Published by**
***THE LAW AND TECHNOLOGY COMMITTEE***
Student Bar Association, National Law School of India University,
Bangalore, India

**Faculty Adviser**
**PROF. RAHUL SINGH**
Assistant Professor of Law, National Law School of India University,
Bangalore, India

IJLT The INDIAN JOURNAL of LAW and TECHNOLOGY

VOLUME 4 2008

## INFORMATION ABOUT THE JOURNAL

The Indian Journal of Law and Technology (ISSN 0973-0362) is a peer-reviewed journal, edited and published annually by students of the National Law School of India University, Bangalore, India. The Journal comprises:

- The Board of Advisory Editors, consisting of professionals and academicians pre-eminent in law and technology, which provides strategic guidance to the Journal.
- The Article Review Board, a panel of external peer-reviewers.
- The Editorial Board, comprising students of the National Law School of India University, which is responsible for selecting and editing content as well as contributing occasional notes and comments.
- The Law and Technology Committee, again comprising students of the National Law School of India University, which publishes the Journal and carries out secretarial functions.

## INFORMATION FOR CONTRIBUTORS

The Indian Journal of Law and Technology invites the submission of articles, book reviews, comments and essays on topics relating to the interface of law and technology, particularly those with a developing world perspective.

- **Mode of Submission**

Manuscripts may be submitted either in electronic form, though electronic submissions are very strongly encouraged.

Please address electronic submission to:
The Chief Editor
Indian Journal of Law and Technology
ijltsubmit@nls.ac.in

Please address hard copies of manuscripts to:
The Chief Editor
Indian Journal of Law and Technology
National Law School of India University,
P.O. Box 7201, Nagarbhavi,
Bangalore - 560 242, India

To facilitate the review of manuscripts submitted in hard copy form, authors are urged to also provide copies of their manuscripts on a recordable compact disc or DVD. It is regretted that the manuscripts cannot be returned to the authors.

- **Regular Submission Review**

The Journal will provide authors with an acknowledgement shortly upon receipt of the manuscript. Preliminary review of submissions will normally be completed within four weeks of submission. Submissions that are initially accepted are double-blind-refereed by the Article Review Board. Efforts will be made to complete the peer-review process within a reasonable time frame, and the Journal will duly notify and update authors regarding the status of the peer-reviews as they are completed.

- **Expedited Review**

Authors who have received an offer of publication (whether conditional or unconditional) from another journal for their manuscripts, may request an expedited review. It shall be at the discretion of the Editorial Board whether to grant an expedited review or not. Please note that requests for expedited review can only be made for electronic submissions. Every such request needs to be accompanied by the following details:

- Name of the author(s) & contact details;
- Title & complete manuscript (compliant with the Submission Requirements below);
- Name(s) and publisher(s) of the journal(s) which has/have accepted the manuscript;
- Whether the offer is a conditional or unconditional offer and, if the offer is conditional what conditions are required to be met for final acceptance;
- The date(s) on which the offer(s) made expire(s);
- Contact information including e-mail address(es) and phone number(s) of the journal(s) that has/have accepted the manuscript.

In completing the expedited review, the Journal will make every effort to accommodate the existing offer(s) and the associated deadline(s). Upon an offer of publication, pursuant to the expedited review, authors will have to communicate their acceptance within five calendar days of notification of the offer; otherwise the Journal will have the discretion to withdraw the offer.

- **Submission Requirements**
  - All manuscripts must be accompanied by:
    (1) a covering letter containing the name(s) of the author(s), the title of the manuscript and appropriate contact information.
    (2) the résumé(s)/curriculum vitae(s) of the author(s).
    (3) an abstract of not more than 200 words describing the submission.
  - Electronic submissions should ideally be made in Rich Text format (.rtf), although Microsoft Word format (.doc), or Open Document format (.odt) are also acceptable.
  - Text and citations must conform to the rules specified in THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia Law Review Ass'n et al. eds., 18th ed. 2004) or a more recent edition thereof. In the latter case, the edition used must be specified in the accompanying covering letter. The Journal employs footnotes as the method of citation.
  - No biographical information or references, including the name(s) of the author(s), affiliation(s) and acknowledgements should be included in the text of the manuscript, file name or document properties. All such information may be incorporated in the covering letter accompanying the manuscripts.
  - The Journal encourages the use of gender-neutral language in submissions.
  - Articles in the Journal will be edited and published according to the orthographical and grammatical rules of Indian English, which is based on British English; thus, submissions in American English will necessarily be modified accordingly and authors are encouraged to use British English for their submissions so as to expedite the review and editing process.
  - One of the reasons the Journal was set up was to encourage debate on issues pertaining to law and technology. Thus, the Journal welcomes articles from a variety of viewpoints, and the content of any article that it publishes should not be taken as an indicator of the ideological leanings of the Journal. Articles that rebut previously published articles or which hold radically different viewpoints are greatly appreciated and will be reviewed on their own merit.

- To facilitate maintaining the highest quality standards and the production of relevant legal scholarship, the Journal strongly encourages authors not to exceed 30,000 words (inclusive of text and footnotes) in their submissions. Submissions of 35,000 words or more will not be considered, barring extraordinary circumstances.
- Authors are required to obtain written permission for the use of any copyrighted material in the manuscript and communicate the same to the Journal. Such copyrighted material may include tables, charts, graphs, illustrations, photographs and block quotations according to applicable law.

- **Copyright**

Upon acceptance, the authors shall grant a licence to edit and publish the manuscript to the Journal while retaining the copyright. Unless otherwise noted, such a license shall be as per a standard terms-and-conditions template that will be provided by the Journal to the authors upon acceptance. The license will inter alia provide the Journal or its assignee(s) with the right to publish the submission in any medium and for both commercial and non-commercial purposes.

## DISCLAIMER

The opinions expressed in this journal are entirely those of the authors and not of the Journal or any other persons associated with it.

## PERMISSIONS

For permission to reprint articles, comments and notes published in the Indian Journal of Law and Technology please contact the Chief Editor by e-mail at ijltedit@nls.ac.in. Alternatively, the Chief Editor may also be contacted at the following address:

The Chief Editor
Indian Journal of Law and Technology
National Law School of India University,
P.O. Box 7201,
Nagarbhavi,
Bangalore - 560 242, India
Email: ijltedit@nls.ac.in

## SUBSCRIPTION INFORMATION

- **Annual Subscription Rates (postage included)**

*Indian Subscribers*

| | One Year | Two Years | Three Years |
|---|---|---|---|
| Students | 200 | 350 | 500 |
| Others | 450 | 800 | 1100 |

*International Subscribers*

| | One Year | Two Years | Three Years |
|---|---|---|---|
| Students | US$25 | US$45 | US$55 |
| Others | US$35 | US$60 | US$80 |

- Demand drafts or cheques for subscriptions may be drawn in favour of 'The Student Bar Association, NLSIU' payable at Bangalore, India.
- Please mention your name, mailing address, occupation, e-mail address, phone number and payment details (cheque/DD no.) on the covering letter.
- Please write 'SUBSCRIPTION' in block letters on the envelope and write your name, address and order details behind the DD/cheque.
- If you are a student, please attach a letter from your institution about your status as proof.
- Please state clearly whether you wish your subscription to begin from the current issue (2008) or from the next issue (2009). In the former case, please allow six weeks for the first issue to be received.
- The previous volumes of the Indian Journal of Law and Technology are available on request. Please contact IJLT at ijltedit@nls.ac.in with any queries.
- If you are an international subscriber who wishes to avail of our special concessions for subscribers from developing countries, please e-mail IJLT at ijltedit@nls.ac.in with the subject 'Developing Country Concessions'.

- **Contact Information**

Please send any queries regarding subscriptions, change of address and related matters by e-mail to IJLT at ijltedit@nls.ac.in. Cheques should be addressed to:

The Librarian,
National Law School of India University,
Nagarbhavi,
Bangalore, 560 242.
India.

For more information and for abstracts of the articles published in previous volumes, please visit the website of the Indian Journal of Law and Technology at http://www.nls.ac.in/students/IJLT.

IJLT The INDIAN JOURNAL of LAW and TECHNOLOGY

VOLUME 4 2008

# CONTENTS

THE INDIAN JOURNAL OF LAW AND TECHNOLOGY
Volume 4, 2008

# SAVING THE INTERNET

*Jonathan Zittrain**

## TABLE OF CONTENTS



## I. INTRODUCTION

The famed Warner Bros. Cartoon antagonist Wile E. Coyote demonstrates a fundamental principle of cartoon physics. He runs off the cliff unaware of its ledge, and continues without falling. The Coyote defies gravity until he looks down and sees that there is nothing under him. His mental gears whirr as he contemplates his predicament. Then: splat!

* Professor of Internet Law, Harvard Law School, and Co-Director, Berkman Center for Internet and Society. 

The Internet and the PC are following a similar trajectory. They were designed by people who share the same love of amateur tinkering as the Coyote, and who dealt with problems only as they arose – or left them to individual users to deal with. This "procrastination principle", together with a design premised on contributions from anyone who cared to pitch in, have caused the Internet and PC to emerge from the realms of researchers and hobbyists, and to win out over far more carefully planned and funded networks and information appliances.

The runaway successes of the Internet and PC with the mainstream public have put them in positions of significant stress and danger. Though the Internet's lack of centralized structure makes it difficult to assess the sturdiness of its foundations, there are strong signals that our network and computers are subject to abuse in ways that have become deeper and more prevalent as their popularity has grown.

The core boon and bane of the combined Internet and PC is its *generativity*: its accessibility to people all over the world – people without particular credentials or wealth or connections – who can use and share the technologies' power for various ends, many of which are unanticipated or, if anticipated, would never have been thought to be valuable.

The openness that has catapulted these systems and their evolving uses to prominence has also made them vulnerable. We face a crisis in PC and network security, and it is not merely technical in nature. It is grounded in something far more fundamental : the double-edged ability of members of the public to choose what code they run, which in turn determines what they can see, do and contribute online.

Poor choices about what code to run – and the consequences of running it – could cause Internet users to ask to be saved from themselves. One model to tempt them is found in today's "tethered appliances." These devices, unlike PCs, cannot be readily changed by their owners, or by anyone the owners might know, yet they can be reprogrammed in an instant by their vendors or service providers (think of TiVo, cell phones, iPods, and PDAs). As Steve Jobs said when introducing the Apple iPhone earlier this year, "We define everything

that is on the phone. You don't want your phone to be like a PC, the last thing you want is to have loaded three apps on your phone, and then you go to make a call and it doesn't work anymore. These are more like iPods then they are like computers."

If enough internet users begin to prefer PCs and other devices designed along the locked down lines of tethered appliances, that change will tip the balance in a long standing tug of war from a generative system open to dramatic change to a more stable, less interesting system that locks in the *status quo*. Some parties to debates over control of the Internet will embrace this shift. Those who wish to monitor and block network content, often for legitimate and even noble ends, will see novel chances for control that have so far eluded them.

To firms with business models that depend on attracting and communicating easily with customers online, the rise of tethered appliances is a threat. It means that a new gatekeeper is in a position to demand tribute before customers and vendors can connect – a discriminating "2" inside "B2C."

## II. TWO GENERATIVE TRIUMPHS: NETWORK AND PC

Some brief history: The mainstream consumer network environment of the early 1990s looked nothing like today's Internet, nor did it evolve to become the Internet we have today. As late as 1995, conventional wisdom held that the coalescing global network would be some combination of the proprietary offerings of the time, services like CompuServe, AOL and Prodigy. Yet those companies went extinct or transformed into entirely different businesses. They were crushed by a baling-wire-and-twine network built by government researchers and computer scientists, one that had no CEO and no master business plan.

The leaders of the proprietary networks can be forgiven for not anticipating the Internet's rise. Not only was there no plan for the provision of content on the Internet, there was an outright hostility towards many forms of it. The Internet's backbone, operated by the U.S. National Science Foundation, had an acceptable-use policy prohibiting commercial endeavors. For years the

Internet remained a backwater, a series of ad hoc connections among universities and research laboratories whose goal was to experiment with networking. Yet what the developers made was a generative system, open to unanticipated change by large and varied audiences. It is this generativity that has caused its great – and unanticipated – success.

Consumer applications were originally nowhere to be found on the Internet, but that changed in 1991, after the Internet's government patrons began permitting personal and commercial interconnections without network research pretexts, and then ceased any pretense of regulating the network at all. Developers of Internet applications and destinations now had access to a broad, commercially driven audience. Proprietary network service providers who had seen themselves as offering a complete bundle of content and access became mere on-ramps to the Internet, from which their users branched out to quickly thriving Internet destinations for their programs and services. For example, CompuServe's Electronic Mall, an e-commerce service intended to be the exclusive means by which outside vendors could sell products to CompuServe subscribers, disappeared under the avalanche of individual Web sites selling directly to anyone with Internet access.

PCs likewise started off slowly in the business world (even the name "personal computer" evokes a mismatch). Businesses first drew upon custom-programmed mainframes – the sort of complete package IBM offered in the 1960s, for which software was an afterthought – or relied on information appliances like smart typewriters. Some businesses obtained custom-programmed minicomputers, and employees accessed the shared machines through dumb workstations using small, rudimentary local area networks. The minicomputers typically ran a handful of designated applications – payroll, accounts receivable, accounts payable, and company specific programs, such as case management systems for hospitals or course-registration programs for universities. There was not much opportunity for skilled users to develop and share innovative new applications.

Through the 1980s, the PC steadily gained traction. Its ability to support a variety of programs from a variety of makers meant that its utility soon outpaced that of specialized appliances like word processors. Dedicated word processors were built to function the same way over their entire product lifetimes, whereas PC word-processing software could be upgraded or replaced with an application

from a competitor without having to replace the PC itself. This IT ecosystem, comprising fixed hardware and flexible software, soon proved its worth.

PCs had some drawbacks for businesses – documents and other important information ended up stored across different PCs, and enterprise wide backup was a real headache. But the price was right, and people entering the workforce soon could be counted on to have skills in word processing and other basic PC tools. As a round of mature applications emerged, there was reason for almost every white collar worker to be assigned a PC, and for an ever broader swath of people to want one at home. These machines might have been bought for one purpose, but their flexible architecture meant that they could quickly be redeployed for many others. A person who bought a PC for word processing might then discover the joys of e-mailing, gaming, or the Web.

Bill Gates used to describe Microsoft's vision as "a computer on every desk". That may have reflected a simple desire to move units – nearly every PC sold meant more money for Microsoft – but as the vision came true in the developed world, the implications went beyond Microsoft's profitability. Whether running Mac or Windows, an installed base of tens of millions of PCs meant that there was tilled soil in which new software could take root. A developer writing an application would not need to convince people that it was worth buying new hardware to run it. He or she would only need to persuade them to buy the software itself. With the advent of PCs connected to the Internet, people would need only click on the right link and new software could be installed. The fulfillment of Gates' vision significantly boosted the generative potential of the Internet and PC, opening the floodgates to innovation.

## III. BENEFITS OF GENERATIVITY: INNOVATION AND PARTICIPATION

Generativity is a system's capacity to produce unanticipated change through unfiltered contributions from broad and varied audiences. As such, generativity produces two main benefits: The first is innovative output – new things that improve people's lives. The second is participatory input – the opportunity to connect to other people, to work with them, and to express one's own ability through creative endeavors.

Nongenerative systems can grow and evolve, but such growth is channeled through their makers; Sunbeam releases a new toaster in response to anticipated customer demand, or an old proprietary network like CompuServe adds a new form of instant messaging by programming itself. When users pay for products or services, they can exert pressure on the companies to develop the desired improvements or changes. This is an indirect path to innovation, and there is a growing body of literature about its chief limitation – a persistent bottleneck that prevents large incumbent firms from developing and cultivating certain new uses, despite the benefits they could enjoy with a breakthrough.

For example, Columbia Law School professor Tim Wu has shown that when wireless telephone carriers control what kind of mobile phones their subscribers may use, those phones often have undesirable features that are difficult for third parties to improve. Some carriers have forced telephone providers to limit the mobile phones' Web browsers to certain carrier-approved sites. They have eliminated call timers on the phones, even though these would be trivial to implement and are much desired by users, who would like to monitor whether they have exceeded the allotted minutes for their monthly plan. These limitations persist despite competition among several carriers.

The reason big firms exhibit such innovative inertia, according to a theoretical framework by Clayton Christiensen, is twofold: Big firms have ongoing investments in their existing markets and on established ways of doing business, and disruptive innovations often capture only minor or less profitable markets – at first. By the time the big firms recognize the threat, they are not able to adapt. They lose, but the public wins.

For disruptive innovation to come about, newcomers need to be able to reach people with their offerings. Generative systems make this possible. Indeed, they allow users to try their hand at implementing and distributing new ideas and technologies, filling a crucial gap that is created when innovation is undertaken only in a profit-making model, especially one in which large firms dominate.

Consider novel forms of commercial and social interaction that have bubbled up from unexpected sources in recent years. Online auctions might

have been ripe for plucking by Christie's or Sotheby's, but upstart eBay got there first and stayed. Craigslist, initiated as a dot-org by a single person, dominates the market for classified advertising online. Web based e-mail, hosting services for personal web pages, instant messaging software, social networking sites and next-generation search engines emerged from individuals or small groups wanting to solve their own problems or try something neat, rather than from firms realizing there were profits to be gleaned.

Eric von Hippel, head of MIT's innovation and Enterpreneurship Group, has written extensively about how rarely firms welcome improvements to their products by outsiders, including their customers, even when they could stand to benefit from them. In his work, von Hippel makes the case to otherwise rational firms that the users of their products can and often do serve as disruptive innovators, improving products and sometimes adapting them to entirely new purposes. They come up with ideas before there is widespread demand, and vindicate them sufficiently to get others interested. These users are commonly delighted to see their improvements shared. When interest gets big enough, companies can step in and fully commercialize the innovation.

We have thus settled into a landscape in which both amateur and professional small- and large-scale ventures contribute to major innovations. Consumers can become enraptured by a sophisticated "first-person shooter" video game designed by a large firm in one moment, and by a simple animation featuring a dancing hamster in the next. So it is unsurprising that the Internet and PC today comprise a fascinating juxtaposition of sweepingly ambitious software designed and built like a modern aircraft carrier by a large contractor, alongside killer applets that can fit on a single floppy diskette. OS/2, an operating system created as a joint venture between IBM and Microsoft, absorbed more than $2 billion of research and development investment before the plug was pulled, whereas Mosaic, the first graphical PC Web browser, was written by a pair of students during a university break.

Generative growth can blend well with traditional market models. Big firms can produce software where market structure and demand call for such enterprise; smaller firms fill in niches; and amateurs, working alone and in groups, can design both inspirational applets and more labor intensive software that increases

the volume and diversity of the technological ecosystem. Once an eccentric and unlikely invention from outsiders has gained traction, traditional means of raising and spending capital to improve technology can shore it up and ensure its exposure to as wide an audience as possible. An information technology ecosystem comprising only the products of a free software movement would be much less usable by the public at large than one in which big firms help sand off rough edges. GNU/Linux has become user friendly thanks to the firms that package and sell copies, even if they cannot claim proprietary ownership of the software itself. Tedious tasks that improve the ease of mastery for the uninitiated are probably best done through corporate models: creating smooth installation engines, extensive help guides, and other forms of hand-holding to help users embrace what otherwise might be an off-putting technical software program or Web service.

For the individual, there is a unique joy to be had in building something-even if one is not the best craftsperson (this is a value best appreciated by experiencing; those who demand proof may not be easy to convince). The joy of being helpful to others – to answer a question simply because it is asked and one knows a useful answer, to be part of a team driving towards a worthwhile goal – is among the best aspects of being human. Our information technology architecture has stumbled into a zone where helpfulness and teamwork can be elicited among and affirmed for tens of millions of people. Novel invention by engineers at the technical layer allows artists to contribute at the content layer. The feeling is captured fleetingly when strangers are thrown together in adverse situations and unite to overcome them – an elevator breaks down, a blizzard or blackout temporarily paralyses the normal cadences of life – but that leads to wonder and camaraderie rather than fear. The internet of the early twenty-first century has distilled some of these values, promoting them without the kind of adversity or physical danger that would make a blizzard fun for the first day but divisive and lawless after the first week without structured relief.

## IV. THE GENERATIVE STALL

Generative technologies need not produce forward progress, if by progress one means something like enhancing social welfare. Rather, they foment change. Generative systems are by their nature unfinished, awaiting further elaboration

from users and firms alike. As such they can be threatened as soon as their popularity causes abusive business models to pop up. The very openness and user-adaptability that make the Internet a creative wellspring also allow for the propagation of assorted evils – viruses, spam, porn, predation, fraud, vandalism, privacy violations and potentially ruinous attacks on Web sites and on the integrity of the Internet itself. This is becoming an existential threat to the generative IT ecosystem.

The benefit of the generative PC is that it may be repurposed by the neophyte user at the click of a mouse. That is also a huge problem, for two main reasons. First, the PC user who clicks on bad code in effect hands over control of the PC to a total stranger. Second, the threat presented by bad code has been steadily increasing. The most well known viruses have so far had completely innocuous payloads. The 2004 Mydoom worm spread like wildfire and affected connectivity in millions of computers around the world. Though it costs billions of dollars in lost productivity, Mydoom did not tamper with data, and it was programmed to stop spreading at a set time. Viruses like Mydoom are more like the crime of graffiti, with no economic incentive, than like the sale of illegal drugs, with its large markets and sophisticated crime syndicates.

There is now a business model for bad code – one that gives many viruses and worms payloads for purposes other than simple reproduction. What seemed truly remarkable when it was first discovered is now commonplace: viruses that comprise PCs to create large "botnets" to open to later instructions. Such instructions have included directing the PC to become the botnet's own e-mail server, sending spam by the millions to email addresses harvested from the hard disk of the machine itself or from Web searches, all in a process typically unnoticeable to the PC's owner. One estimate pegs the number of PC's involved in such botnets at 100 million to 150 million – one quarter of all the computers on the Internet as of early 2007. Such zombie computers were responsible for more than 80% of the world's spam in June 2006, and spam in turn accounted for an estimated 80% of the world's e-mail that month.

Because the current computing and networking environment is so sprawling and dynamic, and its ever-more-powerful building blocks are owned by and managed by regular citizens rather than technical experts, its vulnerability has

increased substantially. The public will not and cannot maintain their PCs to the level that professional network administrators do, despite the fact that their machines are significantly more powerful than the minicomputers of the 1970s and 1980s. That vulnerability is exacerbated by people's increasing dependence on the Internet. Well-crafted worms and viruses routinely infest vast swaths of Internet-connected personal computers. In 2004, for example, the Sasser worm infected more than half a million computers in three days. The Sapphire/Slammer worm in January 2003 went after a particular kind of Microsoft server and infected 90% of them – 120,000 machines – within 10 minutes. These hijacked machines together were performing 55 million searches per second for new targets just three minutes after the first computer fell victim. If any of these pieces of malware had truly "mal" or nefarious purposes – for example, to erase hard drives or randomly transpose numbers in spreadsheets – nothing would stand in the way.

The fundamental tension is that the point of a PC is to be easy for users to reconfigure to run new software, but when users make poor decisions about what new software to run, the results can be devastating to their machines and, if they are connected to the Internet, to countless others. Simply choosing a more secure platform does not solve the problem. To be sure, Microsoft Windows has been the target of malware infections for years, but this in part represents Microsoft's dominant market share. As more users switch to other platforms, those platforms will become appealing targets as well. And the most enduring way to subvert security measures may be through the front door – by simply asking the user's permission to add some malware designed as new functionality – rather than trying to steal in through the back and silently exploit an operating system flaw.

PC and Internet security vulnerabilities are a legitimate menace, and people are right to be concerned. However, the most likely reactions if they are not forestalled will be as unfortunate as the security problems themselves. Users will choose PCs that operate more like appliances, forfeiting the ability to install new code themselves. Instead they will use their machines as mere dumb terminals linked to Web sites that offer added interactivity. Many of these Web sites are themselves amenable to appliance-like behavior. Indeed, what some people have applauded as Web 2.0 – a new form of peer-to-peer networks and collective,

collaborative content production – is an architecture that can be tightly controlled and maintained by a central source, which may choose to operate in a generative way but is able to curtail those abilities at any time.

Consider Google's terrific map service. It is not only highly useful to end users, it also has an open application programming interface to its map data. Thanks to the open API, a third party website creator can start with a mere list of street addresses and immediately produce on her site a Google map with a digital push-pin at each address. This allows any number of "mashups" to be made, combining Google maps with third party geographic data sets. Web developers are using the Google Maps API to create websites that find and map the nearest Starbucks; create and measure running, hiking or biking routes; pinpoint the locations of traffic light cameras; and collate prospective partners on the Internet dating sites to produce instant displays to show where one's best matches are located.

In allowing coders to access its map data, Google's mapping service is generative. But its generativity is contingent: Google assigns each web developer a key and reserves the right to revoke it at any time for any reason – or to terminate the whole service. It certainly is understandable that Google, in choosing to make a generative service out of something in which it has invested heavily, would want to control it. But this puts within the control of Google and anyone who can regulate Google, all downstream uses of Google maps (and maps in general) to the extent that Google Map's excellence means that other mapping services will fail or never be built.

The business model of other next generation Internet appliances and services are neither enduringly generative nor, in some instances, as unambiguously generative as the open Internet and PC. For example, Microsoft's Xbox is a video game console that has as much computing power as a PC and is networked to other users with Xboxes. Microsoft loses money on every Xbox it sells but makes it back by selling its own games and other software to run on it. Third-party developers can write Xbox games, but they must obtain a license from Microsoft (which includes giving Microsoft a share of the profits) before they can distribute them.

Most mobile phones are similarly constrained: They are smart and many can access the Internet, but the access is channeled through browsers provided and controlled by the phone service vendor. Many PDAs come with software provided through special arrangements between the device and software vendors, as Sony's Mylo does when it offers Skype. Without first inking deals with device makers, software developers cannot have their code run on the devices even if the users desire it. In 2006, AMD introduced the Internet Box, a device that looks just like a PC but cannot run any new software without AMD's permission. What's more, AMD can install on the machines any software it chooses – even after they have been purchased.

The growing profusion of tethered applications takes many Internet innovations and wraps them up neatly and compellingly, which is good – but only if the Internet and PC can remain sufficiently in the center of the digital ecosystem to produce the next round of innovations and to provide competition for the locked-down appliances. The balance between the two spheres is precarious, and it is slipping toward the appliances. People buy these devices for their convenience or functionality, and some may appreciate the fact that they limit the damage users can do through ignorance or carelessness. But appliances also circumscribe the beneficial applications users can create or receive from others – applications they may not realize are important to them when they purchase the device. The risk, then, is that users unwittingly trade away the future benefits of generativity, a loss that may go unappreciated even as innovation tapers off.

Eliminate the PC from many dens and living rooms, and we eliminate the test bed and distribution point for new software. We also eliminate the safety valve that keeps information appliances honest. If TiVo makes a digital video-recorder that too strictly limits what people can do with their recorded video, customers will turn to DVR software like MythTV, which records and plays TV shows on PCs; if mobile phones are too expensive, people will use Skype.

Of course, people don't buy PCs as insurance policies against appliances that limit their freedom (even though they serve this vital function); they buy them to perform certain preconceived tasks. But if Internet security breaches and other sorts of anarchy threaten the PC's ability to perform those tasks reliably,

most consumers will not see the PC's merit, and the safety valve will be lost. If the PC ceases to be at the center of the information technology ecosystem, the most restrictive aspects of information appliances will become commonplace.

## V. INFORMATION APPLIANCES AND REGULATION

When information appliances stay connected to their makers, those companies can be asked to implement changes to the way they work long after they have been purchased for a specific use. Consider the case of *TiVo v. Echostar*. TiVo introduced the first digital recorder in 1998, allowing customers to record and time-shift TV shows. In 2004, TiVo sued satellite TV distributor Echostar for infringing TiVo's patents by building DVR functionality into some of Echostar's dish systems, TiVo won and was awarded $90 million in damages and interest – but that was not all. In August 2006 the court issued an order directing Echostar to disable the DVR functionality in most of the infringing units then in operation.

In other words, the court ordered Echostar to kill DVRs in the living rooms of people around the world who had bought them and might be watching programs recorded on them at that very instant. Imagine sitting down to watch a much anticipated TV show or sportscast and instead finding that all your recordings have been zapped along with the DVR functionality itself – killed by a remote signal traceable to the stroke of a judge's quill. The logic is plain: If an article infringes intellectual property rights, under certain circumstances it can be impounded and destroyed. It is typically impractical to go round impounding every item that falls under this category (police officers don't go door-to-door looking for Rolex and Louis Vuitton knockoffs), so plaintiffs and prosecutors traditionally go after only those selling contraband goods. But the tethered functionality of a DVR means that Echostar can easily effect the remote modification or even destruction of its units.

Remote modification can also allow makers to repurpose their appliances, sometimes in ways that are undesirable to their owners. General Motors and BMW offer onboard systems like OnStar to provide car owners with a variety of useful services and functions, including hands free calling, turn-by-turn driving directions, tire pressure monitoring, and emergency roadside assistance. Because

the systems are networked and remotely upgradeable, the U.S. Federal Bureau of Investigation sought to use the technology to eavesdrop on conversations occurring in a vehicle by remotely reprogramming the onboard system to function as a roving bug. The bureau obtained secret orders requiring on carmaker to carry out that modification, and the company complied under protest. A U.S. federal appellate court found in *The Company v. The United States* that the anonymous carmaker could theoretically be ordered to perform the modifications but that the FBI's surveillance interfered with the computer system's normal use. A car with a secret open line to the FBI could not simultaneously connect to the automaker. If occupants tried to use the system to summon emergency help, it would not function (presumably, the FBI would not come to the aid of the motorist the way the automaker promises to do). The implication of the ruling was that secret FBI surveillance of this sort would be legally permissible if the system were redesigned to simultaneously process emergency requests.

A shift to smarter appliances, ones that can be updated by – and only by – the makers, is fundamentally changing the ways in which we experience our technologies. They become contingent: Even if you pay up front for them, such appliances are rented instead on owned, subject to the revision by the maker at any moment.

What price will that control exact? It is difficult to sketch a picture of all the innovative changes that will not happen in a future dominated by appliances, but history offers a guide. Before the generative PC and Internet entered the mainstream around 1995, the IT landscape saw comparatively few innovations. In the dozen years since then, the Internet and PC have combined to inspire accelerated technical innovation outside the traditional firm-based R&D process: new web-powered forms of business value, new social networks and communities of interest, and experiments in collaborative, collective interest. They are crucibles, for new forms of culture, political action and participation, and they will lose their power if the Internet and its end points migrate towards more reliable but less changeable configurations.

## VI. SAVING THE GENERATIVE INTERNET

If the Internet *status quo* is untenable, and the solution of tethered appliances creates too many undesirable consequences, we must look for other solutions. The central challenge facing today's information technology ecosystem is to maintain a generative openness to experiments that can be embraced by the mainstream with as few barriers as possible, in the face of potentially overwhelming problems that arise precisely because it is so flexible and powerful. We may draw useful general guidelines from some of the success stories of the generative model that have shown staying power. Here is a brief sampling.

### A. Netizenship

One solution to the generative problem deploys tools for people to use, usually in small groups, to prevent what they see as abuse. For example, Wikipedia offers easy-to-master tools that make it possible for self-identified editors to combat vandalism that arises from allowing anyone to edit entries. It is a system at once naïve and powerful compared with the more traditional levers of regulation and control designed to stop outliers from doing bad things. It is the opposite of the client-service model in which a customer calls a help line. Rather, it's like a volunteer fire department or neighborhood watch. Not everyone will be able to fight fires or watch the neighborhood – to be sure, some will be setting the fires – but even a small subset can become a critical mass.

The propogation of bad code is a social problem as well as a technical one, and people can enter into a social configuration to attack it. A small application could run unobtrusively on PCs of participating users and report either to a central source, or perhaps only to each other, information about the vital signs and running code of that PC, which would help other PCs understand whether the code is risky or not. With that information, one PC could use other unidentified PCs' experiences to empower the user. At the moment the user is deciding whether to run some new software, the application's connections to other machines could show, say, how many of the other machines were running the code, whether the machines of self-described experts were running it, whether those experts had been moved to vouch for it, and how long the code had been available. It could also signal the amount of unintended network traffic, pop-

up ads, or crashes the code appears to cause. These sorts of data could be viewed on a simple dashboard, letting PC users make quick judgements in light of their own risk preferences.

### B. Virtual Machines

For those people who simply want their PCs to operate reliably, a medium-term solution may lie in technologies that allow mission-critical work to be isolated from whimsical, experimental activities that might be dangerous – or might become the next key use of the Internet. Computer scientist Butler Lamson and others are developing promising architectures that allow single PCs to have multiple zones, two or more virtual machines running within one box. A meltdown in the red experimental zone cannot affect the more secure green zone, and thus the consumer is spared having to choose between a generative box and an appliance. Tax returns and other important documents go in green; Skype starts out in red, and then moves over only when it seems prime time.

### C. More Help from ISPs

Maintaining the security of a generative system is, by its nature, an ongoing process, one requiring the continuing ingenuity of those who want it to work well, and the broader participation of others to counter the actions of a determined minority to abuse it. If the network is completely open, the end points can come under assault. If the end points remain free as the network becomes slightly more ordered, they act as safety valves should network filtering begin to block more than bad code. Today, ISPs turn a blind eye to zombie computers on their networks, so they do not have to spend time working with their subscribers to fix them. Whether through new industry best practices or through a rearrangement of liability requiring ISPs to take action in the most flagrant and egregious of zombie situations, we can buy another measure of time in the continuing cat-and-mouse game of security

### D. Network Neutrality for Mashups

Those who provide content and services over the Internet have lined up in favor of 'network neutrality' by which the ISPs would not be permitted to

disfavor certain legitimate content that passes through their servers. Similarly those who offer open APIs on the Internet ought to be application neutral, so all those who want to build on top of their interfaces can rely on certain basic functionality.

Generative systems offer extraordinary benefits. As they go mainstream, the people using them can share some sense of the experimentalist spirit that drives them. The solutions above are sketched on the most basic of terms, but what they share is the idea that for the generative Internet to save itself, it must generate its own solutions. The more we maintain the Internet as a work in progress, the more progress we can make.

## APPENDIX I: FOUR ELEMENTS OF GENERATIVITY

Four main features define generativity: (1) how strongly a system or technology leverages a possible set of tasks; (2) its adaptability to a set of tasks; (3) its ease of mastery; and (4) its accessibility. The greater extent to which these features are represented in a system, the more readily it can be changed in unanticipated ways – and the more generative it is. For example, many tools can be leveraging and adaptable but are difficult to master – thus decreasing generativity.

**Leverage.** Generative systems make difficult jobs easier. The more effort they save, the greater number of instances in which their use can make a difference to someone, the more generative they are. Leverage is not exclusively a feature of generative systems; non-generative specialized technologies (a plowshare, for instance) can provide great leverage for the tasks they have been designed to perform.

**Adaptability.** Adaptability applies to both the breadth of a system's uses without change and the ease with which it can be modified to broaden its range of uses. Adaptability is a spectrum – a technology that offers hundreds of different kinds of uses is more adaptable, and thus more generative than a technology that offers fewer.

**Ease of Mastery.** How easy is it for broad audiences to both adopt and adapt a technology? An airplane is neither simple to fly nor simple to modify for

new purposes. Paper, on the other hand can be readily mastered and adapted-whether to draw on or to fold into airplanes. The skills needed to use many otherwise generative technologies may be hard to absorb, requiring apprenticeship, formal training or long practice.

**Accessibility.** The easier it is to obtain the technology, tools and information necessary to achieve mastery – and convey changes to others – the more generative the system is. Barriers to access include the sheer expense of producing (and therefore consuming) the technology; taxes and regulations surrounding its adoption or use; and secrecy or obfuscation that its producers wield in order to maintain scarcity or control.

## APPENDIX II: WHAT'S GENERATIVE AND WHAT'S NOT?

**LEGOs and a Dollhouse.** Legos are highly adaptable, accessible and easy to master. They can be built, deconstructed and rebuilt into whatever form the user wishes, and third parties can publish "recipes" for new forms. The less generative dollhouse supports imaginative play, but is itself unmodifiable.

**Hammers and Jackhammers.** A hammer is accessible, easy to master, and useful in any number of household tasks. A jackhammer is less broadly accessible, harder to master and good only for breaking up asphalt, concrete and stone.

**PC and TiVo.** A PC is an adaptable multipurpose tool whose leverage extends through networked access to new software and other users. TiVo is an inflexinle tethered appliance. Though based on the same technology as a PC, it can be modified only by its maker, restricting its uses to those that TiVo invents.

**Bicycles and Airplanes.** Bicycles are accessible (there's no license to pedal), relatively easy to master, and adaptable by large communities of avid users and accessorizing firms. Airplanes are highly useful for long distance travel, but not very accessible, adaptable or easy to master.

THE INDIAN JOURNAL OF LAW AND TECHNOLOGY
Volume 4, 2008

# DATA PROTECTION EFFORTS IN INDIA: BLIND LEADING THE BLIND?

*Latha R. Nair**

## ABSTRACT

*This paper, after establishing the need for effective data protection in India, goes on to describe the rudimentary measures taken in the country till date in the sphere of data protection. While highlighting the inadequacy of such measures and the ambiguity in proposed amendments, the author seeks inspiration from European Union law in proposing a broad framework for data protection law in India.*

## TABLE OF CONTENTS



* Latha R. Nair is a partner at K&S Partners, New Delhi. She may be contacted at latha@knspartners.com.

## I. WHY PROTECT DATA?

The need to protect data and data privacy in India is relatively new, arising from the ever expanding off-shoring business operations conducted in India by overseas companies wherein personal data is exported by these overseas companies to their off-shore agents or counterparts in India.[1] If it was not for this mushrooming off-shoring business, India would perhaps never have worried much about data protection, as there are already existing provisions in the Indian legal framework for protection of data, albeit not at the scale at which protection is warranted under the current circumstances.

Keeping in mind that data is the principal basis of most off-shoring businesses, it would be instructive to examine the intended objectives of any data protection law. For instance, the European Data Protection Directive[2] has as its twin objectives the protection of privacy of individuals with regard to the processing of personal data and, the facilitation of the free movement of such data. The two stated objectives would ordinarily contradict each other, and the task confronting any authority would be to reconcile these objectives by protecting privacy rights, while simultaneously ensuring the free movement of data.[3] In other words, the directive aims to achieve processing of data by maintaining data privacy.

India had been the hot-spot for off-shoring operations for foreign companies for a long time, till concerns of data security were raised, following certain incidents of data theft and breach of data privacy by certain Indian off-shoring

---

1 *See* Jürgen Schaaf and Thomas Meyer, *Outsourcing to India: Crouching Tiger Set to Pounce* (Deutsche Bank Research), Oct. 25, 2005, *available at* http://www.dbresearch.com/PROD/DBR_INTERNET_EN-PROD/PROD0000000000192125.pdf (stating that India is the world's most important offshoring location).

2 Council Directive 95/46, 1995 O.J. (L281) 31 (EC).

3 *See* CHRIS REED, COMPUTER LAW 418 (5th ed., 2004) (explaining how the Data Protection Directive mirrors the 1981 Council of Europe Convention on data protection which attempts to reconcile privacy and the desire to maintain free flow of information between trading nations).

companies.[4] These incidents made headlines in national and international media and brought India's legal framework for data protection under worldwide scrutiny. While India continues to be a hotspot for off-shoring, it cannot avoid data security issues for much longer, as both the industry and the government have been under tremendous pressure to enact a law for data protection in India.

## II. EXISTING LEGAL FRAMEWORK FOR DATA PROTECTION IN INDIA

### A. Contract Law

The existing Indian legal framework for data protection from an off-shoring angle falls mainly under the law of contract. Under the Indian Contract Act, 1872, a company can bind another through a contract to protect the data of the former. This is possible because of the reason that the Act defines 'consideration' as any act or abstention at the desire of the promisor,[5] which means that for certain reciprocal consideration, one firm can bind another so as to refrain from revealing data without authorisation, and foist upon it the positive obligation to protect data. Such a contract may mention the specific duties and obligations of both the parties involved and should have provisions relating to the duty of the Indian company to protect privacy of data, as well as the terms and conditions of the use and processing of data. Currently, all off-shoring operations in India are regulated by such contracts. In a scenario like this, contractual clauses are crucial in order to determine the extent of data security. Most of the time, negotiations by foreign data exporters with Indian companies aim at reaching a balance between maximum business benefits and adequate protection of personal data.

---

[4] *See, e.g., Ex-IITian Arrested for Delhi Call Centre Data Theft*, THE TIMES OF INDIA, Nov. 12, 2005, *available at* http://timesofindia.indiatimes.com/articleshow/1293310.cms.

[5] Section 2 of the Indian Contract Act states that "[w]hen, at the desire of the promisor, the promisee or any other person has done or abstained from doing, or does or abstains from doing, or promises to do or to abstain from doing, something, such act or abstinence or promise is called a consideration for the promise."

## B. The Information Technology Act, 2000

Apart from the Indian Contract Act, 1872, some provisions pertaining to data protection are also present in the Information Technology Act, 2000. The Information Technology Act (hereinafter, "The IT Act") was enacted in 2000 with the main purpose of providing legal recognition to transactions carried out by means of electronic commerce, as has been stated in its preamble. The definition of 'data' in the Act covers a representation of information, knowledge, facts and so on, which are being prepared or processed in a computer system in any form or stored internally in the memory of the computer.[6]

Section 43(b) of the IT Act stipulates penalties by way of damages up to Rs. 10,000,000 against any person who "downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium".

Further, Section 66 of the Act defines 'hacking', and lists the punishment for the same. It reads:

> *66. (1) Whoever, with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.*
>
> *(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with a fine which may extend up to two lakh rupees, or with both.*

The expression "or affects it injuriously by any means" could be interpreted to include a breach of privacy of the data. Hence, although the IT Act primarily provides legal recognition for transactions carried out by means of electronic commerce, there are some provisions dealing with data protection.

---

[6] Section 2 of the IT Act defines 'data' as "representation of information, knowledge, facts, concepts or instruction which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer".

## III. RECENT EFFORTS IN INDIA TOWARDS DATA PROTECTION

Instances of data theft have compelled both the government and the industry to remedy the situation as a response to international pressure, in terms of providing some sort of framework for data protection. Some of these efforts are discussed below.

### A. Proposed Amendments to The IT Act

In view of growing concerns raised by recent instances of data theft, the Ministry of Information Technology proposed certain amendments to the IT Act, 2000. One such amendment, pertinent to data protection, is the proposed insertion of a new Section 43A wherein sensitive personal information would be handled with reasonable security practices and procedures. The proposed amendment reads as follows:

> *43A. Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation not exceeding five crore rupees, to the person so affected.*
>
> *Explanation: — For the purposes of this section,—*
>
> *i) 'body corporate' means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;*
>
> *(ii) 'reasonable security practices and procedures' means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;*

*(iii) 'sensitive personal data or information' means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.*

This has taken the form of Clause 20 of the Information Technology (Amendment) Bill, 2006.

However, nothing in the proposed amendments deals with crucial aspects of data protection such as the processing of personal data, handling of sensitive personal data, the conditions under which data may be collected from an individual, the precautions to be taken while collecting data, confidentiality and security of processing of the data collected and so on.

The proposed amendments have not yet materialised into new provisions under The IT Act and have only recently received the comments of the Standing Committee on Parliamentary Affairs.

## B. The Data Security Council of India

The National Association of Software and Services Companies (NASSCOM) has set up a self-regulatory initiative in data security and privacy protection called the Data Security Council of India (DSCI). What led to the establishment of the DSCI is the continuing effort by NASSCOM to ensure that the Indian information technology industry has a safe environment that can be benchmarked with the rest of the world.[7]

The DSCI is a self-regulatory body established under the premise that the industry, rather than the government, is best positioned to develop appropriate data privacy and security standards as it has greater knowledge and better understanding of the practical commercial issues involved. It is felt that such an approach would allow the DSCI to evolve and effectively respond to global developments. The DSCI would adopt global standards in order to move towards this end, initially focussing on establishing its membership and evolving a code of conduct by promoting a culture of privacy. Initially, the DSCI would promote

---

[7] *See* Data Security Council of India (DSCI), *available at* http://www.nasscom.in/Nasscom/templates/NormalPage.aspx?id=51973.

and encourage voluntary compliance with the code of conduct, gradually creating a mechanism for enforcement of the same in an effort to establish its credibility.[8]

The DSCI is envisaged as a non-profit organisation, with its governing body having an adequate representation of independent directors and industry specialists. Organisations associated with data security and privacy protection such as Information Technology (IT) and Information Technology enabled Services (ITeS) companies, academic or research institutions and universities can also become members of the DSCI.[9]

The DSCI's stated mission seeks to:[10]

- Enable IT and ITeS companies to provide a high standard of security and data protection by adopting best practices.
- Develop, monitor and enforce an appropriate security and data protection standard for the Indian IT and ITeS industry that would be adequate, cost effective, adaptable and comparable with global standards.
- Build capacity to provide security certification for organizations.
- Create a common platform to promote the sharing of knowledge about information security and foster a community of security professionals and firms.
- Create awareness among industry professionals and other stakeholders about security and privacy issues.

## C. National Do Not Call Register

As discussed at the very outset, any data protection law should aim at protecting the privacy of data and, at the same time, ensuring the free movement of data. The issue of privacy of personal data, especially personal telephone

---

[8] *See Data Security Council of India: A Self-Regulatory Initiative in Data Security and Privacy Protection, available at* http://www.nasscom.in/upload/5216/Datasecurity.pdf (setting out the objectives of the Council in the guiding principles).

[9] *Id.*

[10] *Id.*

numbers, has been the subject of great discussion among legal and industry circles in the recent past in India. The multiplicity of telecommunication service providers, coupled with easy and inexpensive mobile phone connectivity has led to rampant breaches of the personal privacy of mobile phone users. Taking advantage of the enormous amounts of freely available mobile phone user data, many industries in the finance, banking, health and tourism sectors have set up telemarketing services to tap the potential business opportunities that lie in such data. Consequently, telemarketing calls have become yet another intrusion introduced by the digital revolution in the lives of Indians, and what initially appeared to be a matter of routine inquiries regarding loans or credit card requirements turned out to be a massive and unabated nuisance to the receivers of such calls.

Eventually, the Telecom Regulatory Authority of India (TRAI) had to take steps to curb these unsolicited commercial calls pursuant to a petition filed by a Delhi-based lawyer before the Delhi State Consumer Dispute Redressal Commission (hereinafter "the Commission") against a leading private telecom company, Airtel, along with two banks, on various counts including breach of privacy, financial loss, mental harassment and agony, and wrongful gain by the respondents. While allowing the petition and passing severe strictures against the respondents, the Commission also directed the establishment of a National 'Do Not Call' Register by TRAI, which would bind all the players in the market, placing special emphasis on the fact that commercial telemarketers could not call a subscriber if their number was on this Register. On the establishment of such Register, subscribers would be called upon to register their telephone numbers free of cost through the Internet by publicising such a Register in the newspapers.[11]

Effective from October, 2007, TRAI put in place the National 'Do Not Call' Registry (NDNC), with the primary objective of curbing unsolicited commercial communication (UCC). The Telecom Unsolicited Commercial Communications Regulations, 2007, defines UCC as, "any message, through telecommunications service, which is transmitted for the purpose of informing about or soliciting or promoting any commercial transaction in relation to goods,

[11] *See Heavy Fines Imposed on Telemarketing Company*, http://news.indlaw.com/guest/databasesearch/articles/core_articledisplay.asp?ID=Unsolicited_focus2.

investments or services which a subscriber opts not to receive."[12] Exceptions to UCC are messages received under a contract, communications relating to charities etc., and communications transmitted under the directions of the government, in the interest of the sovereignty and integrity of India.

The NDNC register will, therefore, be a database containing the list of all telephone numbers of subscribers who do not wish to receive UCC.[13]

## IV. DO THESE EFFORTS BY INDIA SUFFICE?

It is evident from the most recent steps taken by India toward data protection as listed above that there is a strong awareness and inclination on the part of the government and the industry to protect data in India. However, are these steps constructive enough to offer comprehensive protection for data as well as provide the required comfort level to foreign companies to engage in off-shoring business activities in India? Or are they mere baby steps taken in the direction of data protection? The following section aims at examining whether these would, in fact, provide adequate protection to the world's largest back office operations taking place in India.

### A. Amending The IT Act to Protect Data: Fitting a Square Peg in a Round Hole?

Let us first look at the proposed amendments to The IT Act. A reading of the preamble to The IT Act indicates that it is an Act to provide legal recognition to transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as 'electronic commerce' transactions. The preamble does not mention data protection as an objective although one of the purported objectives of the proposed amendments to The IT Act is data protection. Since India's experiences from the inadequacy of data protection in these times of off-shoring are unprecedented and new, it would be useful to look at jurisdictions such as Europe which have existing e-commerce and data protection laws. The member

[12] Telecom Unsolicited Communications Regulations 2007, Regulation 2(q).

[13] *See* National Do Not Call Registry, *available at* http://ndncregistry.gov.in/ndncregistry/index.jsp.

countries of the European Union are also obligated to enact national laws for various areas, including that of data protection and e-commerce.[14]

As part of the harmonisation of the European Union, there are various directives that member countries are required to adopt as their national laws. Two such directives in the areas of data protection and e-commerce are, European Directive 95/46/EC (hereinafter, the "Data Protection Directive") and European Directive 2000/31/EC (hereinafter, the "E-commerce Directive"). The Data Protection Directive was enacted for the protection of individuals with regard to the processing of personal data and the free movement of such data.[15] On the other hand, the E-commerce Directive was enacted with a view to, *inter alia*, contribute to the proper functioning of the internal market by ensuring the free movement of information society services among the member states.[16]

Under Article 2(a) of the Data Protection Directive, 'personal data' is defined as, "any information relating to an identified or identifiable natural person." The Directive is to apply to the processing of personal data, wholly or partly by automatic means, and to the processing of personal data which forms part of a filing system, otherwise than by automatic means. Certain types of processing, such as the processing of personal data for public security, defence, state security, activities in the areas of criminal law and processing by a person in the course of personal or household activities, are exempt from the scope of the Directive.[17]

Under the Directive, member states are under various obligations, including ensuring that data is processed fairly and lawfully, that it is collected for specified and legitimate purposes and not processed in a manner incompatible with those purposes, that the processing of data is adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed and that the data collected is accurate and kept up to date and kept in a form which

---

[14] For instance, the United Kingdom enacted the Data Protection Act in order to conform to EC Directive 95/46/EC, as is evident in the preamble of the Act.

[15] Council Directive 95/46, art.1, 1995 O.J. (L281) 31 (EC).

[16] Council Directive 2000/31, art.1, 2000 O.J. (L178) 8 (EC).

[17] *Supra* note 15, art. 3.

permits the identification of data subjects etc.[18] Further, personal data may be processed only if the data subject has unambiguously given his consent and such processing is necessary not only for the performance of a contract to which the data subject is party but also for the protection of the interests of the data subject.[19]

Besides, the Directive prohibits not only the processing of certain personal data (such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, and health or sex life), but also processing for the purposes of preventive medicine, medical diagnosis, offences and criminal convictions, and so on, except under certain conditions.[20] Further, the data subject must be provided a right to object to the processing of data relating to him and, where there is a justified objection, it must be provided that the processing may no longer involve such data.[21] Apart from being under an obligation to keep the confidentiality of the processing of data,[22] the entity processing the data must also be required to implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, accidental loss, unauthorised disclosure etc.[23]

These are some of the salient features of the Data Protection Directive. It is, therefore, evident that the Directive covers a whole range of issues associated with processing of personal data in keeping with the twin objectives of the Directive, as discussed earlier.

The E-commerce Directive specifically excludes from its purview, issues relating to information society services already covered by the Data Protection Directive.[24] Since its objective is to provide for certain legal aspects of information society services, in particular electronic commerce, the E-commerce Directive stipulates various requirements to be imposed on service providers by member

---

[18] *Id.* at art. 6.

[19] *Id.* at art. 7.

[20] *Id.* at art. 8.

[21] *Id.* at art. 14.

[22] *Id.* at art. 16.

[23] *Id.* at art. 17.

[24] *Supra* note 16, at art. 1(5) (b).

states and required to be complied with by service providers. The Directive requires a member state to ensure that service providers render information such as their names and addresses, along with their electronic mail addresses that allow contact and communication with them in a direct and effective manner, as also details of any public registration or identification number, and so on.[25] Further, it stipulates that commercial communications, which are part of an information society service, comply with certain conditions, such as ensuring that the communication as well as the person making the communication shall be clearly identifiable.[26] Under the Directive, UCC by electronic mail by a service provider established in their territory shall be identifiable, clearly and unambiguously, as such, as soon as it is received by the recipient.[27] Also, service providers undertaking UCC by electronic mail must regularly consult the opt-out registers in which persons not wishing to receive such commercial communications can register themselves.[28] The Directive also exempts intermediary service providers of liability in situations when they are mere conduits,[29] as also in cases of caching[30] and hosting,[31] and stipulates that member states are not to impose a general obligation to monitor the service providers.[32]

Hence, the E-commerce Directive covers issues raised in the context of information society services, service providers, and the obligations of member states and the providers of these services regarding such services.

An overview of both these directives reveals that while the E-commerce Directive deals with all aspects of information society services in detail, the Data Protection Directive deals in detail with one aspect of information society services, namely data protection. Also, while both these directives deal with aspects of information society services, the object and concept of both are distinct and different.

---

[25] *Id* at art. 5.

[26] *Id.* at art. 6.

[27] *Id.* at art. 7 (1).

[28] *Id.* at art. 7 (2).

[29] *Id.* at art. 12.

[30] *Id.* at art. 13.

[31] *Id.* at art. 14.

[32] *Id.* at art. 15.

As India is treading new ground as far as data protection and e-commerce laws are concerned, it would be useful to take a leaf or two out of Europe's experience in establishing a legal framework for data protection. While all data transfers and processing are e-commerce transactions, all e-commerce transactions are not data transfers or processing. This explains why the European E-commerce Directive specifically excludes from its purview issues relating to information society services which are already covered by the Data Protection Directive. Although data protection is part of e-commerce, the implications of protecting data have a wider reach and scope and will have to be dealt with in detail through a separate piece of legislation. By attempting to fit provisions for data protection into The IT Act, comprehensive data protection cannot be achieved. For instance, the proposed amendments would not ensure that data is processed fairly and lawfully, that it is collected for specified and legitimate purposes and not processed in a manner incompatible with those purposes, that the processing of data is adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed or that the data collected is accurate and kept up to date and kept in a form which permits identification of data subjects, that the data subject has unambiguously given his consent in processing data, that adequate measures are taken to ensure data privacy etc.[33]

In fact, such issues arising out of data protection are relevant not only to the off-shoring industry, but also to domestic IT-savvy industries and operations in India. For instance, a recent move by the state of Karnataka, stipulating biometric identification through fingerprints for ration card holders, came in for a lot of criticism from certain activists, who argued that such an extensive database, in the absence of a data protection law, would be intrusive and vulnerable to misuse.[34] Perhaps, the off-shoring business has paved the way for a sort of new awakening to issues of privacy in a country like India, where notions of personal privacy are brushed aside in a cultural milieu of sharing and accommodating.

---

[33] In other words, the proposed amendments would not achieve the wider ends enshrined in the eight data protection principle contained in Article 6 of the Data Protection Directive.

[34] *See* Bageshree S., *Now Biometric Identification for Ration Cards Too*, THE HINDU, Nov. 29, 2007, *available at* www.hindu.com/2007/11/29/stories/2007112954530500.htm.

In this connection, it is also relevant to mention the report of the Standing Committee on Information Technology on the proposed amendments to the IT Act, as well as the recommendations made by it. The Information Technology (Amendment) Bill, 2006 was introduced in Parliament on 15th December, 2006, and referred to the Standing Committee on Information Technology on 19th December, 2006 for examination. On 29th August, 2007, the Committee considered and adopted a Draft Report. It appears from the report that, while there were suggestions for separate data protection legislation from the industry and the Department of Information Technology, there was perhaps not enough consensus, conviction or understanding on the need for the same.[35]

## B. DSCI and NDNC

While the efforts made by NASSCOM in establishing the DSCI are commendable, only time would tell whether the self-regulation of an industry of this sort is a lotus-eater's vision or an achievable dream. The DSCI's stated mission is extremely encouraging in these times, when data security is one of the major concerns for foreign investors in India. The DSCI would have to build up a sufficient membership, with the willingness to comply with its code of conduct, before it can push forward its stated objectives. If and when a data protection law is enacted by India, the DSCI could play a pivotal role in administering such a law. While it is too early to comment on how effective the DSCI is in data protection, it certainly is a positive step in that direction.

The effect of the establishment of the National 'Do Not Call' Register on telemarketing calls has been quite dramatic, in that there has been a remarkable slide in the number of calls to those who took the effort to opt out by registering in the register under the NDNC. Also, as in the case of the DSCI, it is too early in the day to comment on the NDNC's functioning or its efforts to protect data privacy.

---

[35] *See* STANDING COMMITTEE ON INFORMATION TECHNOLOGY, TENTH REPORT, *available at* http://164.100.24.208/ls/CommitteeR/Communication/10rep.pdf.

## V. A CASE OF THE BLIND LEADING THE BLIND OR OF TURNING A BLIND EYE?

All the above Indian endeavors towards data protection, though with the best of intentions, could perhaps be described as a case of the blind leading the blind. Or is it a case of the powers-that-be turning a blind eye to the issue? A reading of the report of the Standing Committee on Information Technology on the proposed amendments to The IT Act concerning data protection makes it clear that while the industry and the legislators are familiar with terms like 'personal data', 'sensitive personal data', 'personal privacy', 'data privacy' and so on, there is a lot of ambiguity as to how these terms should be interpreted for effective data protection in India.[36] Without an in-depth understanding of the industry's needs and what is involved in the protection of data and data privacy in India, all the above efforts will remain mere efforts. Nor would attempts to do patchwork on existing legislation, so as to protect data, meet the current need for a legal framework. Emulating the European example of data protection by distinguishing it from protection of e-commerce transactions would undoubtedly place India on the global map when it comes to data protection. Besides, it would also create a safe environment for foreign companies to invest in India. Till then, it needs to be seen how long the off-shoring industry is going to indulge India's baby steps towards data protection.

[36] *Id.*

THE INDIAN JOURNAL OF LAW AND TECHNOLOGY
Volume 4, 2008

# OF SQUARE PEGS AND ROUND HOLES: TOWARDS A NEW PARADIGM OF DATABASE PROTECTION

*Deepu Jacob Thomas* & Prasan Dhar***

## ABSTRACT

*This article looks at the question of the applicability of copyright law to the protection of databases. It features a detailed discussion of the EU Database Directive, which is the only comparable legal framework for the protection of databases. It then discusses some problems that the EU Directive encounters vis-à-vis public interest concerns, and outline why the EU Directive is unable to strike the right balance, both in principle and in practice. Next, it briefly studies database protection law as it exists in the United States, Australia, Canada and finally India, following which the need for protection of databases in India is assessed. Finally, a basic alternative framework for the legal protection of databases is proposed, seeking to balance the interests of database generators and those of the public at large. The authors argue that databases should be protected with reference to principles of the law of unfair competition, which recognizes that a balance needs to be struck between the interests of owners and the public. The authors also suggest the registration of databases with a governmental authority (similar to the trademark registration process) so as to properly delineate the scope of commercial exploitation that the database owner intends. Further, an argument is made for compulsory licensing provisions.*

* 4th Year Student, NALSAR University of Law, Hyderabad.

** 4th Year Student, NALSAR University of Law, Hyderabad.

## TABLE OF CONTENTS



## I. INTRODUCTION

*"Increasingly, the central question is becoming who will have access to the information these machines must have in storage to guarantee that the right decisions are made."*

**- Jean-Francois Lyotard**[1]

[1] JEAN-FRANCOIS LYOTARD, THE POST-MODERN CONDITION: A REPORT ON KNOWLEDGE 15 (Manchester University Press, 1984).

In his classic treatise *The Postmodern Condition*, Lyotard referred to the phenomenon of the transfer of decision-making from administrators to machines, and also of the concentration of information in the hands of a few. In a certain sense, his apocalyptic vision of capitalism and societal transformation has proved to be prophetic, and it is certainly an issue that ails the information society as it stands today.

Over the last decade or so, the growing importance of raw and applied information in commerce has made the protection of databases a contentious issue across the globe. We live in an 'information society', in which the importance of information is paramount. As Ilkka Rahnasto puts it,[2] in agricultural societies, land was most important; in industrial societies, labour and machines became important; and finally, in information societies, information has become the most important resource.[3]

What has put database protection on the policy agendas of most developed economies (and India's), has been the ease with which technology has allowed the profligate spread of databases (along with their information), and, ironically, a corresponding increase in unauthorised access to these databases. This spread of technology has also increased the ease with which data may be copied. If hard work was ever at any point a deterrent to copying a database, it has suffered a well-deserved rout through the spread of technology coupled with the ubiquitous use of technology for copying and replication. The United States Supreme Court declared over a decade ago that the facts or information within databases or compilations could not be the subject-matter of copyright.[4] Three essential approaches to improve the protection of information have emerged in the past half-century or so, the first based on an absorption of 'low authorship' productions, as it were; the second being a Nordic *sui generis* model based on a copyright model that prevented the wholesale appropriation of data; and finally, a tort-misappropriation model.[5]

---

[2] ILKKA RAHNASTO, INTELLECTUAL PROPERTY RIGHTS, EXTERNAL EFFECTS, AND ANTI-TRUST LAW: LEVERAGING IPRS IN THE COMMUNICATIONS INDUSTRY 50 (Oxford University Press, 2003).

[3] *Id.*

[4] Feist Publications v. Rural Telephone Service Co., 499 US 340 (1991).

[5] J.H. Reichman, *Database Protection in a Globalised Economy*, REVUE INTERNATIONALE DE DROIT ECONOMIQUE - 2/3 (t. XVI) (2002), *available at* http://www.cairn.info/article_p.php?ID_REVUE=RIDE&ID_NUMPU (last visited Nov. 29, 2007).

The European Union, in its efforts to harmonize and provide greater protection for intellectual property in data, passed the EU Database Directive,[6] which allowed the information within a database to be protected under a new *sui generis* right. At a theoretical level, it would be pertinent to look at the reasons for copyright in general versus the copyrighting of databases in particular (in the form of a *sui generis* regime). The underlying rationale of copyright law in general has been to promote the making of creative works. While the idea behind copyright law is to provide an incentive to persons to produce creative works by granting them a monopoly over their product, the idea behind granting a *sui generis* protection to databases is more akin to a 'real' property right (in the Lockean sense). So, we find that the rationale behind database protection is that information is treated as 'property *per se*', as opposed to copyright in general, where it is limited to 'property with a purpose'.[7] Under traditional copyright law, the right in intellectual property was purposive in nature, meaning that the association of the term 'property' with cultural production was merely a fiction to grant protection to works produced by members of society.

The implication of the above discussion leads us to the ultimate question: what, then, is the best way to protect databases? It is evident that the reason behind the protection of a certain interest will significantly affect the manner in which that interest is protected. The idea is that that the notion of originality derives its sustenance from the question of human input.[8] It is from this fundamental thought, despite varying interpretations, that we notice the sense of 'fictionalised property'. It is a reward for input. This is quite separate from treating databases as 'property *per se*'. Copyright and database rights "may have concepts in common but, if so, that is only because those concepts happen to fit, not because a database is a species of copyright."[9] Further, if we understand the distinction between 'fictionalised property', in the realm of copyright, and 'property *per se*', in the realm of database protection, it might lead us to the

---

[6] Council Directive 96/9, March 11, 1996 O.J. (L 77) 20 (EC), *available at* http://europa.eu.int/ISPO/infosoc/legreg/docs/969ec.html (last visited Aug. 15, 2007) [hereinafter *EU Database Directive*].

[7] That purpose being to promote greater works to be produced for the benefit of the public.

[8] Hasan A. Deveci, *Databases: Is Sui Generis a Better Bet than Copyright?*, 12 INT'L J.L. & INFO. TECH. 178, 182 (2004).

[9] British Horseracing Board v William Hill, [2001] RPC 31, §23.

notion that the use of copyright law to protect databases was merely a case of square pegs and round holes (and only as long as the pegs were small enough to fit in the holes).

It seems that if the law vests a right in a person, then it must be in the form of either a property interest or a personal interest, as in the case of a tort.[10] Then, the fundamental jurisprudential judgment must be to choose between a 'property rule' and a 'liability rule', as in that of misappropriation or unfair competition.[11]

## II. THE EU DATABASE DIRECTIVE

The European Union placed itself at the vanguard of the move towards the legal protection of databases with the issuance of the *Directive on the Legal Protection of Databases*,[12] which not only included guidelines for the legal protection of databases, but also enjoined European countries to pass municipal legislation implementing its provisions.[13]

In 1988, the European Commission's *Green Paper on Copyright and the Challenge of Technology: Copyright Issues Requiring Immediate Attention* realised the need for legislation to protect computer databases.[14] Subsequent to the *Feist* case,[15] the EC made a proposal for such protection which was then crystallised into the EU Database Directive,[16] which came into force on January 1, 1998.

---

[10] Raymond T. Nimmer and Patricia A. Krauthaus, *Information as Property – Databases and Commercial Property*, 1 INT'L. J. L. & INFO. TECH. 3, 6 (1993).

[11] J.H. Reichman and Paul Uhlir, *Database Protection at the Crossroads: Recent Developments and Their Impact on Science and Technology*, 14 BERKELEY TECH. L.J. 793 (1999). *See* Guido Calabresi and A. Douglas Melamed, *Property Rules, Liability Rules and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089 (1972) (discussing the idea of property rules/entitlements and liability).

[12] *EU Database Directive*, *supra* note 6.

[13] *Id.* art. 16.

[14] W.K Khong, *National and Inernational Developments on Copyright and Rights in Databases*, 6 MALAYSIAN J. LIB. & INFO. SCIENCE 71, 72 (2001).

[15] Feist Publications v. Rural Telephone Service Co., 499 US 340 (1991).

[16] *EU Database Directive*, *supra* note 6.

The EU Directive defines a database as "a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means."[17] Consequently, the Directive covers compilations of data in both traditional 'hard copy databases' and 'electronic databases'.[18] However, the Directive limits this protection by providing that it would not apply to "computer programs used in the making or operation of databases accessible by electronic means".[19] Such exclusion makes it clear that the protection under this Directive only focuses on the database's structure and the contents contained therein.

The EU Database Directive provides for a dual (or two-tier) system for database protection, comprising:

- Copyright protection for the structure of the database (covering creative databases); and
- S*ui generis* protection for the contents of the database (covering non-creative databases).[20]

These two systems stand independently of each other.

## A. Copyright protection under the Directive

The copyright provisions in the Directive have been placed in Chapter 2. The Directive explicitly notes that "the copyright protection of databases provided for by this Directive shall not extend to their contents and shall be without prejudice to any rights subsisting in those contents themselves."[21] By virtue of this provision, the EU tried to harmonize the scope of copyright protection granted to databases with *sui generis* protection for their contents.

---

[17] *EU Database Directive*, *supra* note 6, art. 1.2.

[18] *Id.* art. 1.1.

[19] *Id.* art. 1.3.

[20] *See* Yijun Tian, *Reform of Existing Database Legislation and Future Database Legislation Strategies: Towards a Better Balance in the Database Law*, 31 RUTGERS COMPUTER & TECH. L.J. 347 (1998).

[21] *EU Database Directive*, *supra* note 6, art 3.2.

The Directive also provides for a common standard of originality. Article 3.1 provides that protection must be afforded to databases if they, "by reason of the selection or arrangement of contents, constitute the author's own intellectual creation."[22] This standard is very similar to the standard of originality set up by the United States Supreme Court in the *Feist case*.[23] This standard of originality,[24] as will be discussed later, is much higher than the 'sweat of the brow' standard followed in most other common law jurisdictions.[25] Consequently, creative originality has become the sole rule by which a database will be entitled to the protection of the copyright provisions of the Directive.[26]

The Directive provides for a set of 'restricted acts' and 'exceptions to restricted acts'.[27] The restricted acts are similar to those under traditional copyright law, and include reproduction, adaptation, distribution, communication and display or performance to the public.[28] The exceptions that have been provided under Article 6.1 of the Directive include mandatory exceptions, which allow lawful users to engage in any restricted act "which is necessary for the purposes of access to the contents of the database and normal use of the contents." Article 15 of the Directive explicitly provides that any contractual provision contrary to the exception mentioned in Article 6.1 shall be 'null and void'.[29] The Directive further provides for certain non-mandatory exceptions, which are:

---

[22] *EU Database Directive*, *supra* note 6, art 3.1.

[23] Feist Publications v. Rural Telephone Service Co., 499 US 340 (1991).

[24] *Id.* at 350.

[25] *Supra* note 19, at 356.

[26] *EU Database Directive*, *supra* note 6, art 3.1. Article 3.1 of the Directive provides that "in accordance with this Directive, databases which, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation shall be protected as such by copyright. No other criteria shall be applied to determine their eligibility for that protection." Some commentators have pointed out that "the Directive requires a 'modicum of creativity' and leaves to the Member State Legislatures and the European Court of Justice, the further development of the creativity standards." *Id. See* Julie Wald, *Legislating the Golden Rule: Achieving Comparable Protection under the European Union Database Directive*, 25 FORDHAM INT'L. L.J. 987, 1007 (2002).

[27] *EU Database Directive*, *supra* note 6, art 6.

[28] *Id.* art. 5.

[29] *Id.* art. 15.

- Reproduction for private purposes of a non-electronic database;
- Illustration for teaching or scientific research;
- Use for the purposes of public security or an administrative or judicial procedure; and
- Other traditional exceptions authorised under national law.[30]

In addition, the Directive also provides a general limitation for the application of all the above exemptions (both mandatory and non-mandatory). It provides that the application of these exemptions should not "unreasonably prejudice the right holder's legitimate interests or conflict with normal exploitation of the database."[31] Even though these exceptions are in existence, as Tian notes,[32] they are narrower than the exceptions under traditional copyright, as the exceptions with relation to criticism, comment, news reporting and personal use in case of electronic databases are missing.[33]

The period of protection provided within the Copyright portion of the Directive is similar to a traditional copyright, which extends to a period of 70 years beyond the death of the author.[34]

### B. *Sui Generis* protection under the Directive

Chapter 3 of the EU Directive contains a property model of database protection which is analogous to, yet quite separate from, copyright protection.[35] It treats a database as property, in respect of which the owner has some exclusive rights and the right to assign, transfer or license those rights.[36] Databases, as has already been mentioned, are defined broadly as "a collection of independent

---

[30] *EU Database Directive*, *supra* note 6, art 6.2(a)-(d).

[31] *Id.* art. 6.2(d)(1).

[32] Yijun Tian, *supra* note 20, at 368.

[33] *Id.*

[34] *EU Database Directive*, *supra* note 6, art 2(c). This article limits the scope of the Directive with respect to the term of the Copyright Protection.

[35] *EU Database Directive*, *supra* note 6, art. 13. *See also* Mark J. Davison, *Sui Generis or Too Generous?*, 21 UNIV. NEW SOUTH WALES L.J. 735 (1998).

[36] *EU Database Directive*, *supra* note 6, art 7.1.

works, data or other materials arranged in a systematic or methodical way and accessible by electronic or other means."[37] The maker of the database, who has made a substantial investment in the obtaining, verification, or presentation of contents, is given two exclusive rights in respect of that database. These are the rights of 'extraction' and 're-utilization'.[38] Article 7(1) provides that the exclusive rights of 'extraction' and 're-utilization' are available to a database maker who shows that "there has been qualitatively and/or quantitatively a substantial investment in the obtaining, verification and presentation of the contents." This is essentially the crux of the *sui generis* right; it does away with any standard of creativity. Originality is no longer a legal concern for the protection of the database. It is sufficient that a quantitatively adducible 'substantial investment' has been made.[39] It is here that we can infer that the status of the information contained in the database is of 'property *per se*', as opposed to 'property with a purpose'.[40]

'Extraction' under the Directive is defined as "the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form."[41] 'Re-utilization' is defined as "any form of making available to the public all or a substantial part of the contents of a database by the distribution of the copies, by renting, by online or other forms of transmission."[42] The right of re-utilization covers making the database available to the public in any form, either by way of an electronic copy or by hard copy. The right of extraction is analogous to the right of reproduction under copyright law. The Directive, however, goes further and provides that even temporary transfer to another medium will be an infringement.[43]

Article 7.5 provides that the database owner can even prevent the repeated and systematic extraction and/or re-utilization of *insubstantial parts* of the database, provided the extraction and/or re-utilization conflicts with the normal

---

37 *EU Database Directive, supra* note 6, art 1.2.

38 *Id.* art 7.1.

39 *Id.*

40 *See generally supra* note 2.

41 *EU Database Directive, supra* note 6, art. 7.2(a).

42 *Id.* art 7.2(b).

43 *Id.*

exploitation of the database and/or unreasonably prejudices the legitimate interests of the owner.[44]

The Directive, in effect, confers perpetual protection over the entire contents of the database, at least as long as the database is updated. Therefore, we find that although under the Directive, the period of protection is limited to 15 years,[45] Article 10 goes on to say that "[T]he right provided for in Article 7 shall run from the date of the completion of the making of the database. It shall expire fifteen years from the first of January of the year following the completion of the database." Now, if this provision were to be read in conjunction with Article 7, it would mean that any change in the database (whether qualitative or quantitative) made by substantial investment would lead to the commencement of a new term. In effect, this would grant perpetual protection to databases. This is especially significant in the case of dynamic databases.[46] Furthermore, this would also mean that protection would exist for those contents of the database that were collected more than 15 years before the newest term of protection.

The exceptions that have been provided under the Directive in relation to the *sui generis* provisions are meagre, especially in light of what we have discussed above regarding the duration of copyright. The provisions regarding the exceptions are vague and provide little indication as to how they are to be interpreted.[47] Let us take an example; Article 9(b) of the Directive allows for states to provide for the extraction of a substantial part of the contents of the database "for the purpose of illustration for teaching and scientific research, as long as the source is indicated and to the extent justified by the non-commercial purpose to be attained."[48] What is interesting is that the scope of protection is defined relatively clearly, but the exceptions are optional for implementing countries, and the scope thereof has been left unclear.[49]

---

44 *EU Database Directive*, *supra* note 6, art. 7.5.

45 *Id.* art. 10.

46 Dynamic Databases are those databases whose contents are constantly updated. So, if a change in a dynamic database amounts to substantial investment, the protection will be renewed on a constant basis.

47 *See* Davison, *supra* note 35.

48 *EU Database Directive*, *supra* note 6, art 9(b).

49 Deveci, *supra* note 8, at 201.

A general critique of the *sui generis* model of database rights is that it generates a monopoly and could lead to the abuse of market position. In the Directive, the fundamental problem is that it allows the abuse of market position for the reason that "investors in database production can always deny third parties the right to use pre-existing data in value adding application."[50] That, then, inherently limits the scope of derivative works, unlike in copyright law,[51] even though the Directive includes a provision that the right granted thereunder cannot be used to facilitate the abuse of a dominant market position. Joanna Wu notes that there is a tension between competition principles and the *sui generis* right.[52] Furthermore, as Reichman puts it, this has potentially snuffed out the idea of a public domain that itself was the justification for granting interests in intangibles, as it were, from the start.[53] Reichman and Samuelson also point out that the most controversial objects of protection, that is raw data or facts, have also, paradoxically, received the maximum protection for any sort of intellectual property.[54]

## III. THE DIRECTIVE BEFORE THE COURTS

Before the definitive judgment of the European Court in *British Horseracing Board v. William Hill Organisation Ltd.*,[55] the interpretation of the EU Database Directive came up before various domestic Courts in the EU. This section will examine the cases that came up in Germany, the Netherlands and Britain.

### A. Germany

The first case that came up in Germany regarding the interpretation of the Directive was *Tele-Info-CD*,[56] where Tele-Info-CD, which was a subsidiary of

---

[50] J.H. Reichman and Pamela Samuelson, *Intellectual Property Rights in Data?*, 50 VAND. L. REV. 51, 81 (2001).

[51] *Id.*

[52] Xuqiong (Joanna) Wu, *E.C. Database Directive*, 17 BERKELEY TECH. L.J. 571, 585-586 (1994).

[53] Reichman, *supra* note 5.

[54] J.H. Reichman and Pamela Samuelson, *supra* note 50, at 94.

[55] British Horseracing Board Ltd v William Hill Organisation Ltd., (C203/02) [2004] ECR I-10415 (ECJ).

[56] Re Unauthorised Reproduction of Telephone Directories on CD-Rom Case, I ZR 99/66 [2000] ECC 433 (ECJ).

Deutsche Telecom (DT), scanned and copied the telephone listings of DT and published them on a CD-ROM. The German Federal Court held in an earlier order that the listings amounted to mere technical organisation, which was dictated by matters of efficiency and expediency. As such, the listings were not covered by the law of copyright. In the meantime, the Directive came into force in Germany, and the Court went on to hold that the listings were covered under the Directive by virtue of there being substantial investment[57] since the contents were arranged systematically,[58] and were capable of being accessed individually, as they were arranged alphabetically.[59]

Another case that came up in Germany concerned the repeated extraction of an insubstantial part of the database. In the *StepStone case*,[60] there were two competing online job agencies. The StepStone website allowed users to search jobs industry-wise as well as geographically. OFIR put out their own job vacancies. However, they also created deep links from their website into StepStone's website. OFIR did not dispute that StepStone's website was a database, but argued that since StepStone's database was accessible to the public, OFIR had an implied licence to deep link, and that additional platforms providing access to StepStone's website were, in fact, beneficial to StepStone.[61] The Cologne County Court held that deep linking, which bypassed StepStone's homepage, amounted to a repeated and systematic use of insubstantial parts of the database, thereby infringing StepStone's rights.[62]

### B. The Netherlands and the Spin-Off Doctrine

In order to protect its database, the database maker must show that it has made "qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents."[63] So the question that

---

[57] Re Unauthorised Reproduction of Telephone Directories on CD-Rom Case, I ZR 99/66 [2000] ECC 433 (ECJ), ¶ 36.

[58] *Id*, ¶ 42.

[59] *Id.*

[60] StepStone v. OFIR.

[61] Hasan A. Deveci, *supra* note 8, at 203.

[62] *Id.*

[63] *Id.*

arose in the Dutch Courts was whether 'spin-off' databases are also entitled to protection under the EU Directive. A 'spin-off' database is essentially one which is the 'by-product' of another main activity of the producer of the database.[64] The initial discussions over the 'spin-off' theory took place in the course of legislative proceedings in the Dutch Parliament during the adoption of the EU Database Directive.[65]

Dutch Courts were divided over this issue. In two cases, *Denda v. KPN*[66] and *KPN v. KSO*,[67] the Courts held that 'spin-off' databases were entitled to protection primarily on the ground that the Directive does not make a distinction between primary and secondary exploitation of databases. They said that it would not make a difference whether or not the investment was made if protection was not granted to the database.[68]

However, in *De Telegraaf v. NOS*,[69] De Telegraaf had copied programme listings from NOS which the latter claimed were protected under the *sui generis* right, so as to publish its own TV guide. The Dutch Competition Authority found that there was no substantial investment in the making of television programmes by the Dutch public and commercial broadcasting organisations. Programme schedules, according to the Competition Authority, were by-products of the programme scheduling process. Therefore, the broadcasters could not invoke database protection under the *sui generis* right, since there was no substantial investment. The case was also being argued before the civil Courts. The Court of Appeal of The Hague, applying the 'spin-off' theory, held that the "broadcasters, whose primary task is to make radio and television programmes, cannot accomplish this task without collecting the data on the programmes and redacting the programme lists" and, therefore, "the mere editing/redacting of the programmes does not show a (specific) substantial investment in time,

---

64 Estelle Derclaye, *Database Sui Generis Right: Should We Adopt the Spin-off Theory?*, 26(9) EUR. INTELL. PROP. REV. 402 (2004).

65 *Id.*

66 Denda v. KPN/PTT Telecom, [2001] AMI 69.

67 Kanttekening bij KPN v. XSO, [2000] 4 Informatierecht/AMI 71.

68 *Supra* note 52, at 404, as cited in S. Gijrath and B. Gorissen, *Applying the Database Act to Online Information Services: A Trial and Error Exercise*, [2000-01] CW 26.

69 De Telegraaf v. NOS/HMG, (1999) 1 AMI 12.

money or otherwise."[70] The Court of Appeal, on this point, specifically referred to the Ministry of Justice's statement in support of its findings. In the *Kranten.com* case, [71] the Court held that a list of newspaper article headings on a website does not represent a substantial investment. The publishers' investment is directed towards the gathering of reports and articles to fill the newspapers. The headlines are invented and do not reflect a qualitative investment. In other words, the Court did not expressly adopt the 'spin-off' theory, but it can be concluded from the judgment that the selection of articles and the drafting of the list of titles to be placed on the websites were a side issue of the business, i.e. publishing printed newspapers.[72]

Clearly, the implication of the above discussion is that the EU Directive, in substance, is fundamentally vague.[73] Indeed, the Database Directive itself does not make any reference to primary or secondary uses of databases.[74]

## C. Britain and the European Court of Justice

The leading case that has come up for the interpretation of the EU Database Directive is *British Horse Racing Board v. William Hill Organisation Ltd.*,[75] which was one of four cases that were referred to the European Court of Justice (ECJ), and then sent back to their respective jurisdictions for final consideration. The aforementioned case affirmed the judgment of the ECJ in *BHB v. William Hill Organisation Ltd.*[76]

The facts of the case are simple. The British Horse Racing Board (BHB) was the regulatory authority for horse racing in England and, in pursuance of its

---

[70] De Telegraaf v. NOS/HMG, [2001] AMI 73.

[71] National Newspapers v. Eureka Internetdiensten V.O.F. and Others, [2000] AMI 205.

[72] *Supra* note 52, at 405.

[73] Xuqiong (Joanna) Wu, *supra* note 52, at 581.

[74] *Supra* text accompanying notes 54 and 55. *See* P. Bernt Hugenholtz, *Program Schedules, Event Data and Telephone Subscriber Listings under the Database Directive: The 'Spin-Off' Doctrine in the Netherlands and elsewhere in Europe* (paper presented at Fordham University School of Law Eleventh Annual Conference on International IP Law & Policy New York, 14-25 April 2003), *available at* http://www.ivir.nl/publications/hugenholtz/spinofffordham.html (last visited Sep. 29, 2007).

[75] [2005] EWCA Civ 863.

[76] (C203/02) [2004] ECR I-10415 (ECJ).

activities, it compiled an extensive database of information on horseracing, which it gathered over a period of time. The BHB also checked whether the horses and the riders met the eligibility requirements to be able to compete in a race. BHB was, therefore, the sole source of the information and the only one to know and confirm the final list of participants in a race. This information was put into a database and was used by a wide variety of users such as racehorse owners, trainers, riders, radio or television journalists and bookmakers. In this case, data was supplied through two channels. First data was made available to a joint venture company between Weatherby's and the Press Association, which forwarded the data to its subscribers in an electronic form called the 'declaration feed'. Following this, one of the subscribers supplied the data to its own subscribers in the form of a so-called 'raw data feed'. These two channels were necessary for punters to place bets. Among the bookmakers was William Hill. William Hill used the raw data feed for its horseracing, bet-making business.

BHB alleged infringement of its *sui generis* database right by William Hill and filed a suit against William Hill in the English High Court, which was decreed. Laddie, J. found that William Hill had violated Articles 7.1 and 7.5 of the EU Database Directive.[77] On appeal to the Court of Appeals, the decision was referred to the ECJ. The ECJ accurately noted the reason for the introduction of the Directive, saying that the idea behind it was to promote the creation of storage and processing systems for already existing materials, and not for the creation of the data itself.[78]

Now, protection for databases is only provided if the maker can show that it has made a quantitatively or qualitatively substantial investment in "obtaining, verifying or presenting" the contents of its database.[79] The Court provided the following guidelines in the interpretation of Article 7.1 of the Directive:[80]

1. "Investment in obtaining" does not mean creating. It does not include resources used for the creation of independent materials. It means investment in *collecting* the information.

---

[77] British Horseracing Board v. William Hill, CA (Civ.Div) [2002] ECC 24.

[78] *Supra* note 65, at 42; *EU Database Directive*, *supra* note 6, Recital 9-10-12.

[79] *EU Database Directive*, *supra* note 6, art 7.1.

[80] BHB v. William Hill Organisation Ltd., (C203/02) [2004] ECR I-10415, 34 -36 (ECJ).

2. Investment in the "presentation of the contents of the database" deals with the resources used for the purpose of giving the database its function of processing information, establishing a systematic or methodical arrangement of the materials contained in the database and organising their individual accessibility. Once again, it does not deal with investment in the creation of the materials contained in the database. This could also take into consideration investments linked with the method used to allow the database to fulfill its main function: the organisation of a set of information to facilitate its access.[81]

3. Investment in "verification" covers those resources used to ensure the reliability of the information contained in the database[82] and to monitor its accuracy. It does not cover resources used for the methodical or systematic arrangement of the materials and the organisation of their individual accessibility. Certification or registration is considered as creation nonetheless, and they are not taken into account.

The Court held that one only needs to fulfill one of the above conditions to secure the right under Article 7.1 of the Directive.[83] With regard to the *BHB case*, the Court held that investment in drawing up the list of the horses and their riders did not constitute investment in the obtaining and the verification of the contents of the database.[84] We can see that by distinguishing between obtaining and creating data, the ECJ has relied on the underlying arguments of the 'spin-off' doctrine, even though the judgment does not explicitly refer to it.[85]

However, the ECJ reiterated in all four cases that the fact of the maker of the database being the same as the creator of the materials within that database does not *prima facie* exclude the database from protection.[86] So, what needs to

---

[81] BHB v. William Hill Organisation Ltd., (C203/02) [2004] ECR I-10415, 37 (ECJ).

[82] *Id.* at 34.

[83] *Id.*

[84] *Id.* at 42.

[85] Mark J. Davison and P. Bernt Hugenholtz, *Football Fixtures, Horseraces and Spin Offs: The ECJ Domesticates the Database Right*, 27(3) EUR INTELL. PROP. REV. 113, 114 -118 (2005).

[86] BHB v. William Hill Organisation Ltd., (C203/02) [2004] ECR I-10415, 46 (ECJ).

be shown by the claimant in such a case is that substantial investment was made in the obtaining, verification *or* the presentation of the contents of the database, independent of the resources used in creating the information in the database.[87] One possible way to get around this situation is for the maker of the contents to create a subsidiary company, license the information exclusively to the subsidiary, and then let the licensee create the database.[88]

With regard to the meaning of 'substantial investment', the ECJ only notes (in the *BHB* case, for example) that the investment required with regard to the obtaining, verification and presentation of the contents of the database was minimal (as opposed to the investment required to create the data).[89]

With regard to the 'substantial part' requirement necessary to constitute infringement,[90] consistent with the approach in traditional copyright law, the ECJ judgment laid down that "it must be considered whether the human, technical and financial efforts put in by the maker of the database in obtaining, verifying and presenting those data constitute a substantial investment."[91] Under copyright law, the requirement of originality determines the scope of the right and the scope of infringement. Only if there is copying of what is 'original' will there be infringement.[92] Therefore, the Court found that there would have been no infringement, as there was no substantial investment in the obtaining, verification and presentation of the contents of the database.[93]

Lastly, with respect to indirect infringement, the Court held that a third party could also commit infringement, but with the qualification that it would not cover cases regarding mere consultation.[94] According to Davison and Hugenholtz, "the best interpretation that can be placed on this part of the judgment is that once a database maker makes its database available to the

---

87 BHB v. William Hill Organisation Ltd., (C203/02) [2004] ECR I-10415 (ECJ).

88 *See* Davison and Hugenholtz, *supra* note 85, at 116.

89 BHB v. William Hill Organisation Ltd., (C203/02) [2004] ECR I-10415, 47 (ECJ).

90 *See EU Database Directive*, *supra* note 6, art 7.

91 BHB v. William Hill Organisation Ltd., (C203/02) [2004] ECR I-10415, 76 (ECJ).

92 Davison and Hugenholtz, *supra* note 85, at 116.

93 *Id.*

94 BHB v. William Hill Organisation Ltd., (C203/02) [2004] ECR I-10415, 57 (ECJ).

public, it is implicitly consenting to the viewing of the database by any person and that consent will cover any temporary copies made for that purpose."[95]

One of the most trenchant criticisms levelled against the ECJ's interpretation of the Directive is that it renders the Directive worthless, since the ECJ distinguished between 'creating' and 'obtaining', and preferred protection only to the latter.[96] Therefore, the possibility of the *sui generis* right being used for protection, especially in view of the weak law of passing-off, would be rather low.[97] Indeed, one scholar has called the judgment "Europe's *Feist*".[98] In relation to the Court of Appeals' interpretation of the ECJ judgment,[99] where the Court mentions that it is the official stamp of approval that changes the nature of data from a mere collection of independent existing materials, it means that any 'official' database would not be entitled to the protection of the EU Database Directive.[100]

Furthermore, the line between 'verification' and 'creation' is still blurred and difficult to locate, though one possible solution may be in noting the time of registration, where verification done after the date of registration will not fall within the scope of the *sui generis* right.[101] Davison and Hugenholtz raise two further questions regarding the decision of the ECJ:[102] first, that the Court did not answer the argument raised by William Hill, which was basically that infringement would only occur if they had copied the 'databaseness' of the database of William Hill, as it already found that the contents taken were not substantial;[103] and second, that the Court failed to lay down any guidelines

---

[95] Davison and Hugenholtz, *supra* note 85, at 117.

[96] *See supra* text accompanying notes 79-81.

[97] Robert Clark, *Database Protection in Europe: Recent Developments and a Modest Proposal*, 7 DATA SCIENCE JOURNAL (2007), *available at* http://www.jstage.jst.go.jp/article/dsj/6/0/OD12/_pdf (last visited Sep. 31, 2007).

[98] Stephen Kon, *BHB/William Hill: Europe's Feist*, 28(1) EUR. INTELL. PROP. REV. 60-66 (2006) (discussing, in part, the similarity between the decision of the ECJ and that of the US Supreme Court in Feist Publications v. Rural Telephone Service Co., 499 US 340 (1991)).

[99] [2005] EWCA Civ 863.

[100] Kon, *supra* note 98, at 65.

[101] Antoinne Masson, *Creation of Database or Creation of Data: Crucial Choices in the Matter of Database Protection*, 28(5) EUR. INTELL. PROP. REV. 261-267 (2006).

[102] Davison and Hugenholtz, *supra* note 85, at 117.

[103] *Id.*

with respect to the term for protection of 'dynamic databases', which could end up being perpetual.[104]

Even so, it is possible that the ECJ realised that the scope of the protection that the Directive grants is extensive and unnecessary, and therefore whittled down the scope of its conferment of rights.

## IV. DATABASE/COMPILATION PROTECTION IN OTHER JURISDICTIONS

Other jurisdictions have not yet legislated any special laws in relation to database rights, whether *sui generis* in nature or otherwise. We can, therefore, briefly review the protection afforded to databases under ordinary copyright law in three important jurisdictions, i.e. the United States, Canada and Australia, before turning to the Indian position in conclusion.

### A. The United States

The landmark case in relation to database protection in the US is *Feist Publications v. Rural Telephone Service Co.*,[105] where the United States Supreme Court held that the telephone listings of Rural Telephone did have the requisite level of originality required for copyright protection. The Court overruled the 'sweat of the brow' doctrine of originality, replacing it with the 'modicum of creativity' standard.[106] The Court further said that copyright law only covered the expression of facts and not the facts themselves, the latter being

[104] Davison and Hugenholtz, *supra* note 85, at 117.

[105] Feist Publications v. Rural Telephone Service Co., 499 US 340 (1991).

[106] The Court believed this doctrine 'flouted basic copyright principles' and failed to satisfy the basic constitutional requirement of originality. Further, the Court stated that "[t]hroughout history, copyright law has 'recognized a greater need to disseminate factual works than works of fiction or fantasy.'... But 'sweat of the brow' Courts took a contrary view, they handed out proprietary interests in facts and declared that authors are absolutely precluded from saving time and effort by relying upon the facts contained in prior works. In truth, 'it is just such wasted effort that the proscription against the copyright of ideas and facts'... [is] designed to prevent." Feist Publications v. Rural Telephone Service Co., 499 US 340, 354 (1991).

unconstitutional.[107] The copyright in a factual compilation, according to the Court, was 'thin'.[108]

Over the years, the Supreme Court, while finding many databases copyrightable[109] due to the low level of creativity required, would hold that there was no infringement as the defendants did not copy the selection or arrangement of information in the database.[110]

Therefore, under copyright law, it is extremely difficult, if not impossible, to protect the information in a database. The other route that might be taken in the US (albeit one that has remained unused) is the law of unfair competition. The evolution of unfair competition concretised into a property-based model in *International News Service v. Associated Press*.[111] The misappropriation doctrine may recognise a property right in the product of one's investment, labour and skill and prevent others from taking that product in a manner that constitutes 'free-riding'.[112] However, this doctrine has been severely limited by *National Basketball Association v. Motorola*,[113] which laid down that information could be only be misappropriated if it was 'time-sensitive'. The US has, so far, made many unsuccessful attempts to legislate on database protection through the *sui generis* route, through a tort/misappropriation model and through a modified competition law model.[114]

---

[107] Feist Publications v. Rural Telephone Service Co., 499 US 340, 471 (1991).

[108] *Id.* at 349.

[109] *See* Kregos v. Associated Press, 937 F. 2d. 700 (2nd Cir, 1991); CCC Info. Serv. v. MacLean Hunter Mkt. Reports Inc., 44 F. 3d. 61 (2nd Cir, 1994). *Per contra*, *see* Matthew Bender & Co. v. West Publishing, 158 F. 3d. 674 (2nd Cir, 1998).

[110] *See* Key Publications Inc. v. Chinatown Today Publishing Enterprises Inc., 945 F. 2d. 509 (2nd Cir, 1991).

[111] 248 US 215 (1919).

[112] Margreth Barrett, INTELLECTUAL PROPERTY: CASES AND MATERIALS 966 (West Publishing, 2003).

[113] NBA v. Motorola, Inc., 105 F. 3d. 841 (2nd Cir, 1997).

[114] For a general discussion on these developments, *see* Philip J. Cardinale, *Sui Generis Database Protection: Second Thoughts in the European Union and What it Means for the United States*, 6 CHI-KENT J. INTELL. PROP. 157 (1996); Lisa Barr, *Database Protection Bill*, 8 DEPAUL-LCA J. ART. & ENT. L. 372 (1997-1998); Jonathan Band, *The Database Debate in the 108th Congress: The Saga Continues*, 27(6) EUR. INTELL. PROP. REV. 205-212 (2005); Charles McManis, *Database Protection in the Digital Age*, 7 ROGER WILLIAMS UNIV. L. REV. 7 (2001-2002).

## B. Canada

In Canada, a database enjoys protection as a compilation under copyright law. There were a number of contradictory cases[115] that came up before the Court, some which took up the 'sweat of the brow' standard,[116] some which picked up the *Feist*-like 'modicum of creativity' standard[117] and others which stood somewhere in between.[118]

The *CCH case*,[119] decided by the Supreme Court of Canada, is now the final word on the law on originality. While there are varying interpretations of the judgment with reference to the level of originality required,[120] the Court emphatically rules that facts are not copyrightable[121] which, in essence, means that the position with relation to the copyrightability of facts remains the same as in the US. So, protecting databases in Canada is also a very tough task under the current legal regime.

## C. Australia

Conversely, in Australia, the standard followed still belongs to the 'sweat of the brow' lineage, which means that facts are copyrightable under the Australian copyright regime. The leading case in this regard is *Telstra*,[122] which was decided by the Federal Court of Australia and later upheld by the High Court of Australia.[123] In *Telstra*, the Australian Courts emphatically rejected the *Feist* standard of creativity and opted for the 'sweat of the brow' approach. This was based on two reasons: first, that unlike the US, where the Constitution and the Copyright Act of 1976 required originality, Australian copyright law

---

[115] For a discussion of these cases and the leading CCH Case, *see* Carys J. Craig, *Resisting Sweat and Refusing Feist: Rethinking Originality After CCH*, 40 UNIV. BOSTON COLLEGE L. REV. 69 (2007).

[116] *See* British Columbia Jockey Club v. Standen, 22 DLR (4th) 467; U & R Tax Services v. H & R Block Canada Inc., (1995), 67 CPR (3d) 257.

[117] *See* Tele-Direct (Publications) Inc. v. American Business Information Inc., [1998] 2 FC 22.

[118] *See* Caron v. Assoc. des Pompiers de Monreal Inc., (1992), 42 CPR (3d) 292.

[119] CCH Canadian Ltd. v. Law Society of Upper Canada, [2004] 1 SCR 339.

[120] For an outstanding discussion of the case, *see* Craig, *supra* note 115.

[121] CCH Canadian Ltd. v. Law Society of Upper Canada, [2004] 1 SCR 339, 355.

[122] Telstra Corp Ltd v. Desktop Marketing Systems Pty. Ltd., [2001] FCA 612 [Fed Ct (Aus)].

[123] DtMS Ltd. v. Telstra Corp., [2002] FCAFC 112.

required no intellectual effort; and second, that the Court noted that the 'originality' requirement was very low, leading to difficulties in applying the standard.[124] Hence, we can conclude that databases and the information contained within them are still the subject of copyright law in Australia.

## D. India

India does not have any separate legislation on the protection of databases. Databases are covered under the Copyright Act, 1956, under the heading of 'literary works'. Furthermore, India followed the common law doctrine of 'sweat of the brow', as was the case in *Burlington Home Shopping v. Rajneesh Chibber*.[125] However, in *Navin J. Desai v. Eastern Book Company*,[126] the Court found that there should be a 'modicum of creativity' involved in a compilation, and therefore denied protection to case-notes published in Law Reports. In another turn, in *Infoseek Solutions v. Kerala Law Times*,[127] the Kerala High Court disagreed with the judgment of the Delhi High Court, keeping in line with the sweat of the brow standard.[128] This dispute now appears to have been settled by the recent Supreme Court decision in *Eastern Book Company v. D.B. Modak*,[129] which effectively endorses the Canadian Supreme Court's decision in *CCH*. This case dealt with the copyright status of legal reports, with special reference to headnotes, footnotes, editorial notes, and other enhancements to the text of court judgments. The Supreme Court followed the Canadian decision in striking a balance between the extremes of 'sweat of the brow' and 'modicum of creativity', holding that creativity is not required to render a work original. What is required is an exercise of skill and judgment, which is seen as a balance between creativity and the mere expenditure of labour and capital.[130]

---

[124] *See* Jacqueline Lipton, *Balancing Private Rights and Public Policies: Reconceptualizing Property in Databases*, 18 BERKELEY TECH. L.J. 773 (2000). For a general discussion about the need for the 'sweat of the brow' requirement in Australia, *see* Sandra Gosnell, *Database Protection Down Under: Would a Sweaty Australia be Better off with a Northerly Change?*, 26 UNIV. NEW SOUTH WALES L.J. 639 (2003).

[125] 1995 PTC (15) 278.

[126] 2002 PTC (25) 641 (Del) (DB).

[127] AIR 2007 Ker. 1.

[128] Shamnad Basheer, *Database Protection in India*, *available at* http://spicyipindia.blogspot.com/2005_11_01_archive.html. (last visited Sep. 31, 2007).

[129] 2008 (1) SCC 1

[130] *See also* Shamnad Basheer, *Are Indian Court Judgments Copyrightable?*, *available at* http://spicyipindia.blogspot.com/2008/01/are-indian-court-judgments.html (last visited Aug. 14, 2008).

Furthermore, the Court emphasized that the protection was extended to those elements that required the exercise of skill and judgment, such as headnotes, editorial notes, and comments such as 'partly dissenting', 'concurring', etc. It did not extend to clerical corrections, syntax corrections, and other work deemed to be merely clerical. This decision will be important in determining the extent of database protection in India. Indeed, if the Supreme Court's endorsement of the *CCH* decision is taken to its logical conclusion, the protection of databases will be a difficult task. However, the applicability of the decision to databases is not yet clear.

## V. A PROPOSAL

The questions that need to be answered are, simply, who or what one wants to protect and for what reasons.[131] To put it differently, the idea is to identify a pressing need to protect a certain interest in a certain way. Database legislation should be in pursuance of an institutional framework that seeks to entrench the notions of competition, fair use and other related public interests, while rewarding investment of database generators. We can summarise certain arguments that have been made regarding a change from *status quo* under different regimes. The underlying idea behind all these arguments is that the proprietary interests in databases must be balanced against the free flow of information. That is to say, the benefits to society in the absence of database rights must be less than those available in the presence of a regime of database protection.[132] One argument that is certainly made in 'modicum of creativity' jurisdictions is that the protection awarded to databases is too little, as the US Supreme Court (in *Feist*) pointed out that facts are not copyrightable.[133] Although no empirical evidence has been put forth to show that databases, in fact, need protection, proponents argue that providing databases with protection will encourage investment in such databases.[134] Even so, others argue that the lack of empirical evidence of an existing market failure in relation to databases

[131] *See generally* Lipton, *Supra* note 124.

[132] McManis, *supra* note 114, at 26.

[133] Feist Publications v. Rural Telephone Service Co., 499 US 340 (1991).

[134] *See* Lipton, *supra* note 124.

makes it difficult to ascertain the need for the regulation of database rights.[135] Interesting counter-arguments that have been made try to prove that databases are sufficiently protected under the law of misappropriation, reverse passing-off, technological protection measures and contracts. In common law jurisdictions, where the 'sweat of the brow' standard still applies, the argument against the *status quo* has tried to show that this originality standard provides protection that is too strong.[136]

It is argued by some that empirical evidence suggests that the EU is dragging its feet with regard to modifying the *sui generis* right,[137] as the positive economic impact of the Database Directive remains unproved.[138] Further, it is argued that a *sui generis* right, combined with unfair competition law, technological protection measures and restrictive licensing, will lead to market domination, resulting in distortions in the market.[139] Reichman and Uhlir argue that it makes the creation of secondary markets, with respect to the information contained in the database, prohibitive in terms of costs.[140] The scientific community fears that the cost of scientific research would surge upward.[141]

It is also interesting to note some of the prerequisites of the protection of information as proposed by Wendy Gordon;[142] These are that the incentive to invest should be defended when: (1) the costs of developing an information product are high; (2) the costs of copying are low; (3) copying yields a substantially identical product; (4) which a copyist can price cheaply, not having substantial research and development costs to recoup; and (5) when consumers,

---

[135] J.H. Reichman, *supra* note 5.

[136] *See* Paula Baron, *Back To the Future: Learning from the Past in the Database Debate*, 62 OHIO ST. L.J. 879 (2001).

[137] Cardinale, *supra* note 113 (discussing Financial Times Columnist James Boyle's criticisms of the Database Directive).

[138] *DG Internal Market and Services Working Paper: First Evaluation of Directive 96/9/EC on the Legal Protection of Databases*, Commission of the European Communities, Brussels 24 -26 (December 12, 2005), *available at* http://europa.eu.int/comm/internal_market/copyright/prot-databases/prot-databases_en.htm.

[139] McManis, *supra* note 114, at 25.

[140] *See* J.H. Reichman and Paul Uhlir, *supra* note 11.

[141] *Id. cf.* Andrew Lawler, *Database Access Fight Heats Up*, 27 SCIENCE 1074 (1996).

[142] J.H. Reichman and Pamela Samuelson, *supra* note 60.

believing the two products are substantially identical, decide to purchase the cheaper one, thereby inducing market failure because the first-comer is unable to recoup its expenses; and (6) such a market failure could have been averted by a period of protection that would allow the first-comer to recoup its expenses and justify its investment in developing the information product.[143]

India's position has been elucidated in a study conducted by WIPO in 2002.[144] Interestingly, the study notes that 80% of the data generation in India is by government agencies.[145] This is possible due to the myriad functions and activities performed by an erstwhile socialist state. Much of the scientific data produced in India also comes from government-run institutions as, till recently, most specialist research institutes in various fields were run by the government. However, this is set to change, especially following the information technology boom in India and increasing private R&D in pharmaceuticals and genetics. The study notes that most private database companies are in favour of database protection.[146] Although the study elucidates the extremely strong protection that databases already receive under copyright law, the Information Technology Act, 2000, and the proposed change to the Copyright Act, introducing protection of technological protection measures, the study also boldly proposes the adoption of the EU Database Directive as a model for protection.[147] In this context, it is in India's interest to have a balanced legislation protecting databases and replacing the existing system of protection.

What we propose in this context is a law that takes certain elements from trademark law and the law of unfair competition. The idea of taking these specific elements, as will be made clear, is to ensure that the form of protection in databases relates more to a liability rule rather than to a property rule and, in that sense, it will try to get around the problem of square pegs and round holes.

---

[143] *Id.*

[144] *A Study On The Impact Of Protection Of Unoriginal Databases On Developing Countries: Indian Experience*, WIPO SCCR/7/5, *available at* http://www.wipo.int/edocs/mdocs/copyright/en/sccr_7/sccr_7_5.pdf. (last visited Nov. 29, 2007).

[145] *Id.* at 8.

[146] *Supra* note 142, at 15.

[147] *Id.* at 29.

The idea is first (and in concomitance with Lipton)[148] that database protection should be limited only to those databases which are intended to be put to commercial use. It is possible that questions may arise relating to mixed uses of a database, i.e. when the purpose of the database is both scientific and commercial. In such cases, protection should be afforded, for at the end of the day, the purpose is commercial, even if only partially.

Second, to enforce the factum of commercial use, the law should mandate that the database is actually put to commercial use in a specific period of time. The effect of non-commercialisation of the database should result in the database being denied protection under law. Lipton, however, considers and denotes her model as a proprietary system.[149] The ill-effects of a proprietary system may not be reflected in legislation, as the dismissal of an 'in-effect proprietary' model pays little heed to the way judges construe legislation. That is to say, the conferment of property-type rights in databases changes the whole basis of protection. What that does, in effect, is direct judges to construe law so as to protect property where the scope and strength of protection is necessarily greater than where one imposes liability rules. The notion of information as property is inherently problematic.[150] Subliminal and sub-legislative directions can influence decisions greatly by providing them the necessary justification for increasing the strength of protection, if the basis of protection were proprietary. In fact, Lipton says that her model is an 'addition' to intellectual property law, in the sense that it comes into play only where other forms of intellectual property protection fail. This may very well be plausible in the US, where, after the *Feist* decision, the protection granted to databases is thin. However, in common law countries, where protection is already very strong, the need is to properly streamline intellectual property policy which may (and we propose that our suggested model does) *supplant* the current law, and does not supplement or complement the existing law.

This, then, leads us to the question of limiting the scope of protection. In relation to infringing conduct, the law should prohibit only that use of the

---

[148] *See* Lipton, *supra* note 124.

[149] *Id.* at 832.

[150] *See generally* Alfred C. Yen, *Western Frontier and the Feudal Society?: Metaphors and Perceptions of Cyberspace,* 17 BERKELEY TECH. L. J. 1207 (2002).

database that will contribute to a decrease in the potential market share of the database, that is to say, that infringing use must be commercial use. Therefore, two conditions should be satisfied in relation to infringing conduct: first, that the infringing conduct must be commercial; and second, that such commercial use must have a potential adverse effect on the market share of the existing claimant database. The idea behind the first condition is to balance and bring into consideration the interests of the scientific and educational communities. The idea behind the second is to ensure the interests of value-adding and downstream commercial users. Obviously, the second condition should be exempted for copying the databases of information providers *per se*. Information providers limit their services to data generation only. But again, if such providers should prove to enter into downstream uses themselves, then we revert to the original conditions of infringing conduct, or possibly deny the database protection altogether in relation to that downstream use as a stricter measure. Therefore, this specifically relies on the model of unfair competition. It is interesting to note that there are three reasons why the EU did not adopt the unfair competition model.[151] First, that a model that is based on unfair competition does not create transferable economic interests.[152] Second, that it only applies to a competitor and not a user otherwise considered.[153] Third, unfair competition laws are not uniform across the EU.[154]

In the case of sole-source information generators and other cases where raw data is very difficult to get, there should necessarily be a compulsory licensing provision. This is necessary to ensure that abusive and oppressive licensing terms are not evolved by such information providers. The grounds could be similar to those provided under patent law.

The third idea is to create a register of databases, similar to that proposed by Lipton[155] and Mazumder,[156] that is managed by a registration body. Two

[151] Stephen M. Maurer, *Across Two Worlds: Database Protection in the US and Europe* 28 (paper prepared for Industry Canada's Conference on Intellectual Property and Innovation in the Knowledge-Based Economy, May 23-24, 2001) as cited in Xuqiong (Joanna) Wu, *supra* note 52, at 575.

[152] *Id.*

[153] *Id.*

[154] *Id.*

[155] *See* Lipton, *supra* note 124.

[156] Anirban Mazumder, *Information, Copyright and the Future*, 29(5) EUR. INTELL. PROP. REV. 180, 186 (2007).

things need to be clarified here: first, the nature and functions of the registration body, and second, the incidents of the registration. The purpose of this will become clear after the following explanation. The registration body or, alternatively, a Registrar, can possibly be of the same nature as that of the Registrar of Companies under the Companies Act, 1956.[157] The function of the Registrar in this context is to ensure that the database so registered is not a database copied from another one (therefore denying the protection of the database law to those who have copied the data) and to administer compulsory licensing terms. In terms of registration, the owner will have to specify the class under which he wants to register his database at the time of registration, as is done in the case of trademarks. The class can be dependent on the intended commercial use of the database. The class ought to be specific, and the owner should be able to register his database in more than one class, provided the regulator has the power to strike down the registration in a particular class if the owner does not exploit it within a reasonable time. This is to prevent owners from uselessly and frivolously registering claims for intended commercial use. The effect of registration would be such that after registration, the owner would be protected against unauthorised copying which would result in any loss of actual or potential market share. This is provided the database using the copied information falls within the same class. Therefore, at the time of registration, owners will have to be careful and register the database in all classes in which they propose to exploit the data. This requirement is necessary to limit the scope, to prevent abuse of a dominant position and to encourage innovation in secondary markets. The data in the protected database can be used by secondary market players, where the use does not affect the actual or potential market of the database owner, provided the owner has not registered his database in that class as well. In fact, the ECJ has held that the abuse of a dominant position may arise where copyright is used to prevent the development of a new, value-added product for a secondary market, not offered by the right holders themselves.[158] Secondary market players will also be able to demonstrate that a

---

[157] Registrars of Companies (ROC) are defined in Section 2(40) of the Companies' Act, 1956 as *"a Registrar, or an Additional, a Joint, a Deputy or an Assistant Registrar, having the duty of registering companies under this Act."*

[158] Daryl Lim Tze Wei, *Regulating Access to Databases Through Antitrust Law: A Missing Perspective in the Database Debate*, 31 STANFORD TECH. L. REV. 7 (2006)

value-added product is being provided via their activities. Like in the *IMS case*,[159] such grounds involve that:

- The product protected by copyright must be indispensable to compete in the secondary market;
- The refusal to license copyright must prevent the emergence of a new product for which there is a potential consumer demand;
- The refusal must not be justified by objective considerations; and
- It must be likely to eliminate all competition in the secondary market.[160]

## VI. CONCLUSION

Any responsible database protection measure must take into account the customary practices of scientists and knowledge-sharing.[161] Such practices are intrinsic to the continuance of our information society. Indeed, in an information society, information is both consumed as well produced by such communities. Also, in an age of digital technology, there are two reasons why digital technology will contribute to a revolution in value-added uses of databases. First, digital technology has the potential to disaggregate the value-added functions of databases,[162] and second, that digital technologies can bring to the fore completely different kinds of functions altogether.[163] A combination of the need to protect and the need to preserve, as it were, questions our fundamental assumptions about the notion of property and the requirement for protection of data.

India's status as a new information economy seems to necessitate database regulation. Our participation in an international framework for such protection

---

[159] IMS Health GmbH & Co. OHG v. NDC Health GmbH & Co. KG, (Case C-418/01) [2004] ECR I-5039.

[160] *Ibid*, at 38.

[161] J.H. Reichman and Paul Uhlir, *supra* note 11.

[162] J.H. Reichman and Pamela Samuelson, *supra* note 50, at 125.

[163] *Id.* at 125.

cannot be limited to simply being a consumer of models that are in force in other jurisdictions. India must take into account the pitfalls that accompany enacting similar proposals. As already noted, the WIPO study proposes that India adopt a similar regime to the *sui generis* regime adopted in the European Union.[164] As a matter of information policy, it is necessary for the government to involve discussions from various stakeholders. We hope that the model that we have suggested might provide one of many starting points for discussion. Importantly, policy makers and legislators must realise that intellectual property reform does not always mean addition, but may sometimes mean substitution, even if that substitution lessens the protection already available. Indeed, as Lawrence Lessig notes,

> *"Overregulation stifles creativity. It smothers innovation. It gives dinosaurs a veto over the future. It wastes the extraordinary opportunity for a democratic creativity that digital technology enables."*

[164] *See supra* text accompanying notes 141 onwards.

THE INDIAN JOURNAL OF LAW AND TECHNOLOGY
Volume 4, 2008

# BOOK REVIEW

*Thomas Schultz,* ***Information Technology and Arbitration: A Practitioner's Guide****, Kluwer Law International, 2006, Paperback.*

*Promod Nair**

Arbitration has often been promoted as providing a faster and more cost-effective dispute resolution alternative as compared to traditional litigation. Yet, complicated procedural motions, discovery disputes and multi-day hearings have resulted in arbitration increasingly replicating formalistic court-like procedures. Users of arbitration fear that excessive "judicialisation" or "legalisation" of arbitration could render the supposed benefits of arbitration rather illusory. While this is inevitable to a certain extent considering the increasing complexity of disputes submitted to arbitration, many of the advantages of arbitration over other forms of dispute resolution can be reclaimed by adopting measures targeted at increasing the efficiency of the arbitral process.[1]

Information technology (IT) tools can help address many of the recent complaints levelled against arbitration by reducing the time and costs of arbitral proceedings. The use of IT aids in arbitration could substantially enhance the efficiency of arbitration – without, it must be stressed, sacrificing procedural guarantees or affecting the quality of justice. For instance:

(i) Online filing sites can provide convenient, safe and reliable repositories for all documents filed in an arbitration;

---

* Associate, International Arbitration Group, Herbert Smith LLP, London.

1 This issue has engaged the attention of the ICC which has set up a Task Force on Reducing Time and Costs in Arbitration which has prepared a succinct report setting out a large number of techniques that could be used in organising arbitral proceedings and controlling their duration and cost. See *Techniques for Controlling Time and Costs in Arbitration- Report from the ICC Commission on Arbitration* (2007).

(ii) E-mails can provide a reliable, fast and secure means of party-tribunal communications;

(iii) Videoconferencing provides an alternative to traditional in-person hearing when such a hearing would be disproportionately expensive, inconvenient or impractical; and

(iv) Realtime transcription tools enable transcripts of hearings to be immediately accessible to all participants at a hearing, which may then be used to cross-examine witnesses or experts.

The last decade has seen the legal world engage with IT in a way never seen before, and although the use of IT in arbitration is still in its infancy, one can sense a perceptible shift of momentum in this regard. Three of the world's leading arbitral institutions, namely the International Court of Arbitration of the ICC, the AAA, and the Arbitration and Mediation Centre of the WIPO have in the last couple of years focussed on increasing the efficiency of arbitral procedures with IT solutions. Without over-egging the pudding, it would be safe to say it appears inevitable that the emergence and development of IT tools for dispute resolution will radically change the conduct of commercial arbitration in the near future.

In this context, a work addressing the manner in which IT solutions can enhance the quality of arbitration proceedings, is of huge relevance to the arbitration practitioner. Thomas Schultz, the author of two previous books on information technology in dispute resolution[2], seeks to address a number of issues concerning the interface between IT and arbitral processes in *Information Technology and Arbitration*:

- The arguments in favour of greater reliance on IT in arbitration;
- The various forms of IT that are available and suitable for use in arbitration, as also the manner in which they could, or are, being used in arbitral proceedings;

---

[2] *Online Dispute Resolution: Challenges for Contemporary Justice* (with Gabrielle Kaufmann-Kohler, Kluwer Law International, 2004) and Réguler le commerce électronique par la résolution des litiges en ligne (Bruylant and L.G.D.J., 2005).

- The main concerns relating to the use of IT in arbitration – the security and efficiency of reliance on IT solutions, and their implications for the procedural rights of the parties; and

- The institutionalisation of IT in arbitration by their incorporation in arbitration agreements and procedural orders.

These issues find detailed examination in the seven chapters of the book, where the author focuses on examining the virtues of "commonplace IT solutions" such as discussion lists, online filing, case management websites, real time transcription software, videoconferencing and even e-mails. The author also looks at the current state of play in the use of these IT tools by the leading arbitral institutions.

Chapter 1 is an introductory chapter that traces the general evolution of IT usage in dispute resolution, and discusses the general benefits of using IT solutions to improve the conduct of arbitral proceedings.

Chapter 2 then looks at the most significant IT tools that are likely to be most widely used in arbitration, namely case management websites (or virtual case rooms), video-conferencing, live note applications used by court reporters which allow a complete reproduction of verbal exchanges to be contemporaneously accessible on computer screens in real time, and global ODR platforms. The coverage of video-conferencing (pp.34-63) is particularly comprehensive and thorough. The technology underlying each tool is discussed, alongwith an explanation of its properties and uses. The author also finally discusses the main issues and concerns raised by each tool, especially in their impact on the procedural rights of the parties.

Chapter 3 provides an overview of how the arbitration world has taken advantage of IT tools to date and surveys the current usage of IT at the ICC, the AAA and the Arbitration and Mediation Centre of the WIPO. It also summarises the ICC's guidelines on the use of IT in arbitration.

Chapter 4 contains an analysis of the main issues that IT usage raises with respect to arbitration law, particularly due process issues and the preservation of confidentiality. Violation of due process rights constitute grounds for annulment

of an arbitral award, and the author discusses potential irregularities that an arbitral tribunal should steer well clear of in adopting IT tools in the arbitral process.

The rest of the book (Chapters 5,6 and 7) set out practice guidelines to be used as a convenient reference tool in practice. It also addresses concerns of legal practitioners in relation to the use of electronic communication technologies in arbitral proceedings.

Schultz is no advocate of technological overkill, and adopts a balanced approach in recommending a simple three-fold test to evaluate the usefulness of technology in any given context:

(a) Does the use of IT tools make the process more effective, i.e., is the quality of the outcome enhanced?

(b) Does recourse to IT make the process more efficient, i.e., does it lead to an appreciable reduction in cost and/or expense?

(c) And lastly, does the use of IT improve convenience?

It is only when the answer to one or more of the questions is in the affirmative that recourse to IT solutions would be beneficial.

Although more of an academic scholar than a practitioner, the author acquits himself admirably in producing a practitioner's guide that is resolutely practical in its approach. The book handles a challenging topic in a clear and accessible manner, with anecdotes and interesting examples enlivening the text. The author has also taken pains to make the book accessible to "ordinary" lawyers, and not particularly to lawyers who are computer buffs.

The book succeeds in its stated aim of providing the arbitration community with an informed insight into the IT toolbox available to make arbitration more efficient and effective, and is hence recommended as a useful read for arbitration community. I heartily concur with Prof. Gabrielle Kaufman-Kohler's endorsement in the foreword to the book, when she comments that the author:

> *"does an outstanding job of providing the arbitration practitioner with good reasons to resort to IT solutions, while offering sufficient advice for everyone to make up his or her own mind about which type of technology to use in a given situation and providing useful considerations on the way to use them."*

Sooner rather than later, parties will expect more than mere legal expertise from their counsel and arbitrators – they would also expect them to operate with maximum efficiency by recourse to state-of-the-art techniques and technologies. This book is therefore an invaluable attempt to help legal practitioners gain adequate awareness of the advantages and stumbling blocks of IT in their practice.