Revisiting E-Courts in India: a bird's eye view from the Australian context

Afroza Begum

American International University, Bangladesh, afroza@uow.edu.au

Publication Details
Revisiting E-Courts in India: a bird's eye view from the Australian context

Abstract
With the advent of globalisation and rapid technological advances, India's response to an electronic court filing system ('e-court') is relatively new. It is only in 2006 that low cost e-filing has been made available to the public by Indian courts. Although this transition facilitates a more sophisticated means of conducting court business and promotes public understanding of judicial proceedings, it has (as elsewhere in the world) caused significant controversy. Some of the controversy surrounds issues about whether the existing infrastructure and socio-economic reality of India can support the move towards electronic courts; whether prevailing laws incorporate an appropriate approach to balance the right to a fair trial and individual privacy concerns; whether e-filing provides desirable aids to reflect judicial credence and public confidence in the administration of justice; and finally, whether e-courts ensure accurate management and reporting of court records. The article aims to explore some of these issues and in doing so, considers Australia's experience with e-courts to see if it may provide any insights into India's contemporary concerns.

Disciplines
Arts and Humanities | Law

Publication Details
Revisiting E-court in India: A Bird’s Eye View from the Australian Context

Afroza Begum *

* LLB (Hons) and LLM (Bangladesh), LLM (Western Sydney), PhD (University of Wollongong, Australia), Professor of Law, American International University-Bangladesh; formerly part-time teaching academic, Faculty of Law, University of Wollongong, Australia; former Member of the National Parliamentary Committee, The Peoples’ Republic of Bangladesh.

Abstract: With the advent of globalization and rapid technological advances the India’s response to e-court is relatively new. Only it is in 2006 that the e-filing has been made available to the public with less charges by the Indian courts. Although this transition facilitates a very sophisticated means of conducting court business and promotes public understanding of the judicial proceedings, it has as elsewhere in the world caused significant controversies. Some of the controversies surround issues as to whether the existing infrastructure and socio-economic reality support the move towards electronic court; whether prevailing laws incorporate an appropriate approach to balance the right to fair trial and individual privacy concerns; whether e-filing provides desirable aids that reflect judicial credence and public confidence in the administration of justice and whether it ensures an accurate management and reporting of the court records. The paper aims to explore some of the issues by briefly looking at Australia’s experiences with e-court that could provide an important insight into the Indian concerns today.

1. Introduction

In attempts to make justice less expensive and burdensome, more accessible and speedy the e-filing in the Supreme Court (SC) commenced in India from 2 October 2006.¹ This electronic innovation gained a strong recognition through its subsequent endorsement in the e-court project approved by the government of India in February 2007.² As part of this process, the National Informatics Centre (NIC) has been entrusted with the responsibility to implement the entire project in three phases which is scheduled to be completed by February 2009. Hence, the stage is in embryonic form negating the

---

feasibility of a critical assessment of e-court’s credibility and effectiveness in India. No readily available statistics exist either to show the e-case records dealt with by the SC of India. Yet, some of the serious concerns have already been raised that fundamentally relate to the e-readiness of the court, the lack of appropriate and adequate infrastructure of the Information and Communication Technology (ICT), the level of protection of privacy issues offered by the existing legislation regarding electronically transmitted and stored data and the security and safety of various ICT Platforms.³ This paper attempts to address these concerns by placing special emphasis on privacy issues in India as compared to Australia. Detailed exploration of the ICT security is however, beyond the scope of this paper as it would be undesirable and even unwise as a layperson in this area to suggest that exactly what standards should be adopted in India to meet the current needs and values given the unanimous and international character of the ICT. The following discussion begins with the e-readiness of the court which reflects some technical and social issues.

2.1. E-readiness of the Court and Social Issues

Certainly, the introduction of the information technology to the court proceedings benefits stakeholders in many ways and arguably outweigh the much discussed debate about the need for maintaining a strict balance between the right to open trial and some fundamental values such as privacy and security of the individual.⁴ In the Indian context, back-log of cases and the disadvantages of maintaining and navigating these through vast amounts of papers and files have been central factors for decades to frustrate the timely

---
disposition of cases. The E-court project aims at redressing the situation by interlinking all the courts across the country which would also help the litigants to have faster access to the proceedings. The project provides step-by-step guide online by which only ‘Advocate-on Records’ and Petitioners-in-person can lodge application and other courts documents electronically. There has been a great body of substantial literature and academic commentaries worldwide to suggest that e-filing and proceedings improve the court’s efficiency and transparency and public confidence in the judicial management.

E-court enables judges to have updated information about the status of particular cases regardless of their location and provides litigants with timely remedies with low cost and less procedural complexities. From that point of view, obviously, the e-court project of India is an appreciable move for the first time in the sub-continent towards a progressive approach to the judicial practice. The important issues are, however, whether the court itself is properly trained up or equipped with necessary IT support to use and accommodate the technology, whether litigants are aware and acquainted of the knowledge and usability of the ICT, whether the entire process is acceptable or understandable by the wider community and whether the available resources support the

---


6 Revolutionary E-court n 1; S Krishnamurthi, National Conference on Legal and Judicial Reforms-the Bird’s Eye View on Balance Sheet and Projections (6-7 September 2002).

7 Supreme Court of India at [http://www.supremecourtofindia.nic.in](http://www.supremecourtofindia.nic.in)


9 Krishnamurthi 2002 n 6; Curtis 2005 id; Security Issues n 4.
sudden replacement of the traditional paper-based courts in India given a number of its socio-economic and specific cultural phenomena.

A total of 15,000 courts situated in approximately 2,500 court complexes are currently operating throughout India.\(^\text{10}\) Essentially, as e-filing, recording, storing and publishing on-line warrant a lot of expertise and IT knowledge, all participants including lawyers, judges, litigants and relevant court officials in judicial proceedings must be familiar with those technologies and knowledge. Accordingly, all IT facilities should also be made available to them before making the e-court fully functional. Although a three months training program under the project initially includes a number judicial officers and court staff at the district level, there is no clear guidelines for the ‘Advocate-on Records’ who are responsible for filing cases as to what professional standards and legal obligations they have to meet in dealing with electronically petitioners’ claims and relevant information.\(^\text{11}\) Some specific mechanism therefore should be in place to provide technolegal education and facilities for all concerned to ensure an accurate electronic management and publication of court records. Developing a strong judicial database incorporating institutional capacity building for all participants and particular methods for the court management from filing to the final disposition of cases with appropriate access policy should have been received careful attention to the e-court project. Even though justice GC Bharuka, the SC of India and Chairman of e-committee, in an interview with

---

\(^{10}\) Revolutionary E-court n 1; ‘Towards Speedy, Inexpensive, Transparent and Accountable Justice’
http://egovonline.net/interview/interview-details.asp.

\(^{11}\) Revolutionary E-court n 1.
E-gov Magazine assured that the Indian Judiciary has all the requisite elements for its institutional capacity building, IT experts refuted the claim.\textsuperscript{12}

In particular, the acceptability of the e-court project by the wider community and its desirability at the present context another issues need to be settled suggesting that the e-service must be usable and affordable by the people. Despite significant progresses in several areas India’s socio-economic reality is still characterized by a traditional culture with deep social disparity, low literacy, sex segregation, discrimination and by the lack of IT knowledge and awareness.\textsuperscript{13} A survey revealed that only 1.2\% of the population in India as compared to 49.3\% of Singapore and 52.5\% of Australia can use online service, and 0.45\% as compared to 46.46\% in Australia has PCs.\textsuperscript{14} This fundamental issue requires to be addressed urgently as the underlying spirit of e-court project appears to implement IT service from top to the grass root level.

\textbf{2.2. Lack of IT Infrastructure and Security}

ICT has a profound contribution to India’s economy and technological advancement which ‘demonstrate a degree of innovation’ in India but the ways it functions have ensued serious controversy over the safety and security of IT platforms. Strong arguments favour the view that India is heading towards a very weak and vulnerable IT base, and it does not have adequate ICT platforms to host and activate the proposed electronic transition. A number of cyber security experts ‘have been warning of the

\begin{footnotes}
\item[14] Ibid.
\end{footnotes}
vulnerability of critical infrastructure like power, transport and water system to malicious hackers’, ¹⁵ and recommends some specific measures for India which include:

(i) technology building blocks for creating, monitoring and managing secure, resilient and always available information infrastructures that link critical infrastructures,
(ii) risk assessment and contingency planning for interconnected transport or energy networks and
(iii) modeling and simulation for training of concerned officials and manpower. ¹⁶

The Information Technology Act 2000 is the sole law in India to deal with Internet safety and security. The Act provides a legal framework for securing online records by introducing, inter alia, public and private key programs, encryption technology and digital signature.¹⁷ It has empowered the government to prescribe ‘control processes and procedures to ensure adequate integrity, security and confidentiality of all records’ ¹⁸ in respect of digital signature. Provisions are also in place for a certifying authority to issue digital signature certificate. Apparently, these provisions are of high standards and are consistent with international practices but may not be effective in dealing with various issues associated with cyber crime given its boundless and complex nature. With these provisions, for example, the law enforcing agency still may experience difficulties in establishing the identity of the criminal. For security purposes anti-viral software, firewall, a wide variety of software and hardware encryption programs, restrictive security policies and self-regulation are commonly available technology employed by different nations. In addition to these, some jurisdictions have developed code-based

---

¹⁶ Ibid.
¹⁷ See The Information Technology Act 2000 ss 3, 5, 10, 14.
¹⁸ Ibid s 10.
regulation and specific security policies denying or limiting search and logging on line.\textsuperscript{19} ‘The Australasian Legal Information Institute (AUSTLII), for example, prevents indexing of its database by other websites and places it databases outside the permitted scope of web ‘crawler’ ‘robot’ or ‘spiders’.\textsuperscript{20}

3. E-court Project and Privacy Issues in India

The e-court of India aims to promote information gateways between courts and public agencies and departments that would facilitate case flow management, online accessibility and availability of legal resources to the Judges, lawyers and public at large.\textsuperscript{21} The project makes it mandatory for the litigants to disclose their personal details as a requirement for the registration of cases online. Pursuant thereto, some states have adopted video technology for hearing and collecting evidence from remote areas. Certainly, these moves facilitate ‘cost-effective’ justice, public understanding of the judicial proceedings and are compatible with the principles of open court.\textsuperscript{22} With these transitions, however, the e-court, as no exception has been made in the project for certain uses, removes all the \textit{de facto} difficulties in accessing judicial records of the traditional paper-based courts what is commonly described as ‘practical obscurity’.\textsuperscript{23} Access to the traditional paper-court records is limited by time, money, location and the inconveniences involved in manually searching process which also lead the concerned court officials with their professional expertise and obligations to consider whether these records should be

\begin{itemize}
\item \textsuperscript{19} See for example, Security Issues n 4; Curtis 2005 n 8; Internet Regulation In Other Countries\textsuperscript{http://www.opennetinitiative.net/studies/china/}.
\item \textsuperscript{20} Curtis 2005 id.
\item \textsuperscript{21} E-court project n 2.
\item \textsuperscript{22} Security Issues n 4.
\item \textsuperscript{23} Curtis 2005 n 8.
\end{itemize}
accessed. These practical impediments arguably work as a safeguard for individual privacy in the paper-court that the e-court now intends to relinquish by enabling public to gain an ‘unprecedented and unfettered control’ over electronically stored data which eventually has raised some obvious concerns. Most of the concerns are linked to the confidential and sensitive information of the parties and the resulting vulnerability of the disadvantaged victims, which became magnified by some socio-cultural prejudices unique to India. The concerns are whether there is any fundamental policy reason to provide public access to court records and if there is any as to what extent that should be desirable and what protection are in place in India to preserve individual privacy. The following discussion focuses on these issues.

3.1. Balancing Right to Fair Trial and Right to Privacy

The right to fair trial is a constitutional imperative in India which necessitates the court proceedings to be open and accessible to the people. The underlying rationale entitles individuals to participate in these state-run institutions to appraise their roles, transparency and accountability towards community. This is also led by a consideration that the open court is fundamental to public knowledge of law that capacitates them to take part in the law making and reforms process. Also, public access to court records contributes to promote social standards for peace and security; the accused and the public are more likely to be discouraged from doing inappropriate conduct when the records and punishment are published and easily accessed. This conception very often even defies the

---

25 Security Issues n 4; Cannon 2004 n 8; Judges Technology Advisory Committee, Model Policy for Access to Court Records in Canada (hereinafter Model Policy).
27 Brenner n 8.
assessment of damaging consequences of open trial on the accused which has been built on a perception that ‘criminal reduces their right to privacy upon commission of a crime’. More importantly, judicial openness is thought to be imperative to place a check on the courts’ power and to advance public respect in the judicial administration. From the judges’ perspectives too, public participation is considered valuable to measure their sophistication of legal knowledge and creativity to meet the contemporary concerns and values of the society.

Based on these assumptions, the e-court project of India allows electronically compilation of personal information and relevant records of disputes and public access to these. Yet, the supposed benefits of the e-court need to be carefully calculated against the potential risks that are likely to be exposed in India. Electronically stored court records, for example, attract and ease public interference much more than the paper-based court to view matters that an individual may wish to keep secret. Unlike paper records, the electronic data can be readily obtained by a simple search and is easier to compile, retrieve and manipulate in an exclusive-cum-novel way. The greater availability of and easy accessibility to information increase the potential for its misuse in the form of data mining, identity theft, harassment and so on. A series of negative consequences of e-court as revealed in different research studies are: the risk of interception of important data; individuals’ incapacity to dominate the way their personal information is used and disclosed; continued embarrassment and trauma of the accused even long after his/her

---

26 Ibid.
29 Kitajima 2000 n 8 at 568.
30 E-court project n 2.
31 See generally Model Policy n 25.
32 Cannon 2004 n 8.
33 Kitajima 2000 n 8 at 570.
34 Id at 566.
punishment; the aggrieved party or victim’s vulnerability to repeated threats by the accused.35

Another crucial point to note is that the e-court must not frustrate the core tenet of justice in advancing speedy trial as the goal of the judicial administration is ‘justice’ rather than ‘speed’.36 Consideration is also needed how the e-process would impact on the litigants and the public. As Lederer argued: ‘[at] some point, too expeditious a proceeding may discourage settlement; easy dissemination of information may make it more difficult to retrieve and correct erroneous multiple data entries; and our citizens might reject as cold, unfeeling, and unfair remote data and testimony.’37 Despite these negative factors, it would be, however, unjust to suggest for the rejection of e-court benefits to uphold the ‘privacy-only-concerns.’ It would not be desirable either to undermine other important values such as individual dignity and privacy to give way an ‘unfettered access’ to records to exploit the benefits of e-court. Hence, a balancing approach must be in place which will search for a modern approach to dealing with contemporary concerns of the judiciary while preserving privacy of the individual. Now let’s look at what balancing approach is available in the legal and administrative framework in India and whether this is appropriate to mitigate the concerns resulted from the e-court.

3.2. Protecting Privacy under the Legislative and Administrative Initiatives of India

There is no specific Act in India to exclusively deal with privacy issues, however, a range of legislation provides protection for individual privacy which include the Constitution of India, the Penal Code, the Information Technology Act (IT Act) 2000 and the Personal

---

36 F Lederer, The Courtroom as a Stop on the Information Superhighway http://www.courtroom2.net/About_Us/Articles/AUSTLREF.HTML.  
37 Ibid.
Data Protection Bill 2006. Article 21 of the Constitution, for example, guarantees that ‘[no] person shall be deprived of his life or personal liberty except according to procedure established by law’. Nevertheless, the existing interpretation of this provision does not provide sufficient basis for embarking upon privacy threats generated by the e-innovation. Similarly, the criminal and civil sanctions are in place to dealing with fraud, negligence, defamation in relation to an intentional disclosure of sensitive information. Yet, these are becoming increasingly inept to investigate and establish these offences primarily for two reasons: the complex and ‘open’ nature of electronic data and the sophistication of public knowledge to use the information technology and; the failure of law to set a standard for judicial or concerned officials in handling electronic materials.38

To regulate different transactions and communications through electronic channels and to address cyber crimes the IT Act was enacted in 2000. The Act, for the first time, attempts to recognize privacy invasion originated from Internet communication by providing a range of protections against an unauthorized access to information.39 The breach of confidentiality and privacy are addressed under section 72 which restrains users who have legitimate access to e-records from disclosing any correspondence, information, document or other materials without the consent of the person concerned, and the violation of this will give rise to a criminal action.

Another attempt was made to protect privacy from undue publication in 2006 by introducing a Personal Data Protection Bill in the Indian Parliament. The Bill permits


39 Section 43, for example, provides protection against unauthorized access to, downloading, extraction, copying of data by imposing penalties up to one core rupee. Article 65 states that whoever knowingly or intentionally conceals, destroys or alter any computer source code shall be punishable with imprisonment up to three years or with fine which may extend up to two lakh rupees, or with both.
different organizations to collect personal information for particular purposes but restricts its use for commercial activities.\(^4^0\) It entitles individuals to claim compensation or damages due to an unauthorized use or disclosure of the personal details, and the data controllers have been proposed to administer the matter as well as the implementation of the Bill.

These two primary laws, however, are flawed in a number of fundamental points. Neither of these set provisions for some important issues relevant to electronic publication such as a definite security policy, the test of due diligence, private defence and internet censorship which, in large part, diminish their guarantees for protection.\(^4^1\) In particular, there is no clear indication in laws of what information is suppressed from publication, what choices are open for the litigants in terms of the disclosure of their confidential information and what possible remedies are available for disregarding those choices. Most significantly, these laws are basically concerned with more generalized electronic communications conducted by different agencies rather than by the courts.

Similarly, the government’s e-court project while places special focus on the potential benefits of e-technology in the judicial administration, unbelievably, fails to recognize any privacy threat or other damaging consequences that may result from online publication. More core issues in relation to e-court such as access policy, security measures, duties and rights of the participants and the court management remain beyond the scope of the project. Available literature does not suggest either that the government undertook any assessment task surrounding all aspects of e-court before making an effort

\(^{4^0}\) Ibid.
\(^{4^1}\) Data Protection Law n 38.
to implement that. Nevertheless, such an assessment was not only desirable but essential
to India given its particular socio-economic background and cultural identities which as
mentioned are still featured by unequal power relations, a rigid demarcation between men
and women, rich and the underprivileged and by deeply rooted other traditional factors.
In such a situation, the electronic ‘unfettered publication’ can have dangerous implication
for many who are vulnerable targets of the influential. The incidents are too numerous to
detail here that the aggrieved parties and witnesses have often been forced and even
brutally killed to withdraw the cases and statements respectively. One study illustrated
the intensity of the problem by revealing that a total of 34 witnesses of Best Bakery case
were taken hostage. Repeated threats by the accused to her life and honour forced the
main witness of the case to withdraw her statement.42 ‘After a trial that lasted for more
than a year, the trial court acquitted all the 21 accused because of lack of evidence.’43
The study demanded for a comprehensive witness protection program and a new judicial
approach which will keep the identity of witnesses confidential throughout the trial,
conduct a closed door trial and avoid exposure of the witness to media. Thus, the
resulting reality even from the traditional paper-court obviates the need for inquiring
possible threats of the e-court to human security and dignity with more care and
sensitivity.

42 Sultanat conducted a study in which she demonstrated how brutally the witnesses were treated by the
accused, and unveiled fundamental flaws in the existing judicial system with particular reference to the
witness protection program. According to the study, ‘Zahira Sheikh, the prime witness in the Best Bakery
case, turning hostile, along with 37 out of the 43 other witnesses. Zahira, the daughter of the Best Bakery
owner witnessed the barbaric killing of 14 people, which included employees of the bakery and members of
her family …[the incident is] said to be the worst of its kind in the history of independent India, gained
notoriety due to the overt support and complicity of the state machinery in the riot. See for details, A
http://www.ipes.org/India_articles3.jsp?action=showView&kValue=1168&keyArticle=1015&status=artic
43 Ibid.
Also, the risk should be assessed by taking into account perceived security threats after trial which is another concern remain unresolved under the current law. In another context, as the e-court facilitates open pleading with litigants’ all personal information including medical and work history, family problems and other details associated with, for example, harassment and sexual offences, it may have negative impact on all litigants regardless of disadvantaged or advantaged. Victims, especially those of sexual offences are more likely to be emotionally intimidated further through electronic publicity.

Hence it seems logical to suggest that the e-court project should develop a more practical approach integrating, inter alia, an effective program to identify and assess the risk and management of e-court, a strong access policy restricted by logging or other search technicalities, the professional and legal standards for court officials in dealing with sensitive information, programs aiming at raising awareness among lawyers, litigants and other participants about their rights and responsibilities, which are categorically addressed at the last part of the paper.

However, it is important to acknowledge here that a rigid application of such an approach may defeat the purpose of the open court. Yet, some legitimate exceptions to the open court, or restrictions imposed by specific policies are well recognized and practiced across nations, and that should be for above reasons. Essentially, the underlying rationale for open court does not demand all case history or materials to be made public.\textsuperscript{44} The disclosure, for example, medical reports and detailed description of sex offences may be essential to reach a fair judgment but that appear to have less or no relevance to satisfying the principles of open court. Again, maintaining a strict balance between privacy and the open trial is neither possible nor practicable but rather a flexible approach is desirable.

\textsuperscript{44} Kitajima 2000 n 8 at 568.
which will minimize the apparent losses emerged from a thorough assessment of the two. In so doing, consideration should be given to, inter alia, the socio-cultural particularities in determining whether privacy or open court should get preference in some circumstances. However, it must not be confused here that the issue is not with the justification for open trial or with allowing or prohibiting public access to it rather with its cautious application to redress growing privacy invasion. Thus, the judgment of such a preference would not diminish the existence of the other; instead will promote a viable route in which both will survive not by producing harm but by ensuring mutual respect. The following section briefly outlines ways how privacy is protected in Australia that could provide an important impetus for dealing with e-court in India.

4. Protecting Privacy in Australia and Some Lessons for India

Privacy is protected in Australia through a range general laws and privacy laws backed up by numerous principles and guidelines of the federal and state governments. Among these the Privacy Act 1988 (cth) (the Act), Privacy Amendment (Private Sector) Act 2000, Legal Practice Act, the Doctrine of Legal Professional Privilege, Information Privacy Principles (IPPs) and National Privacy Principles (NPPs) associated with Guidelines are more important in dealing with personal information used in the electronic channel. While Australia and ACT government agencies are to comply with IPPs, NPPs apply to private sector organizations.45 These laws and principles in general permit disclosure of personal information to the extent of what is consistent with the expectations of the person or is in the public interest.46

The Act provides ways the different organizations should gather, use, preserve and
disclose personal details and entitles individuals to oversee how these are dealt with by
them. The Act empowered the Office of Privacy Commissioner to investigate and resolve
complaints of privacy assault made by individuals and to issue guidelines for regulating
the use and disclosure of personal information.47 These Guidelines aim to assist federal
and ACT government agencies to develop best privacy practice and comply with the Act
in relation to their websites.48 IPPs comprises 11 guidelines seek to promote ‘the best
practice’ and to ensure the prevention of disclosure of personal information at a
reasonable standard. Principle 1, for example, allows the collection of information for a
purpose which is necessary and lawful and is directly related to the function or activity of
the collector. Under Principle 4 a record-keeper who contains personal information is
required to ensure reasonable levels of security safeguards against unauthorized access,
use, modification and disclosure of the information.

The Privacy Amendment (Private Sector) Act 2000 including ten National Privacy
Principles (NPPs) obligate private sectors to develop and implement their voluntary
practice codes in conformity with international standards in handling individual sensitive
and personal information.49 Principle 5, for example, mandates organizations to take
reasonable steps to let the user know the nature, purpose and the legal proceeding of
using or disclosing information. Principle 8 focuses on anonymity providing that
individuals must have the option of not identifying themselves for lawful and practicable
reasons when entering transactions with an organisation.

47 Ibid.
48 Guidelines for Federal and ACT Government Websites
49 Data Protection Law n 38.
Significant protection from an unauthorized publication was offered further through an amendment to the Supreme Court Act. *The Supreme Court Act* 1986 (Vic), for example, necessitates the court to refrain from publishing the whole or part of a proceeding which would ‘...endanger the physical safety of any person, offend public decency or morality, cause undue distress or embarrassment to the complainant in a proceeding.’

Personal information is also protected by the Doctrine of Legal Professional Privilege (DLPP) which regulates the transmission of necessary documents and many communications between lawyers and clients. The legal practitioners, subject to a few exceptions, are under a common law duty of care to act in the best interest of their client, and to ensure a reasonable standard of security and privacy in maintaining confidentiality of client’s information. Failure to do so will result in several actions. In addition, the *Legal Practice Act* 1996 (Vic) provides an important safeguard against abuses by obliging legal practitioner to destroy old client documents and information after seven years.

Despite the sufficiency of laws and principles to ensure adequate standard of protection for privacy in Australia, confusions have emerged over their effectiveness in dealing with personal information in the e-court. Numerous studies identified some common abilities of these laws to control misuses of online publication which are: (i) difficulties in regulating online materials in an indefinite geographical and jurisdictional boundaries; and (ii) difficulties in employing and activating a national mechanism. Some of the

50 *The Supreme Court Act* 1986 ss 18 1(c) and 19.
51 Security Issues n 4.
52 Ibid.
53 Ibid.
54 Ibid.
55 Ibid; Curtis 2005 n 8.
terms frequently used in the provisions of law also create problems in identifying and executing e-irregularities. ‘Reasonable standard’ for example, is a relative word subject to an in-depth analysis and judgment, and therefore is not easy to locate and establish in a unique way. For the same, the judgment tends to leave scope for controversy from which a uniform and definite standard is very hard to achieve.

In particular, a series of exception and exemption clauses, to some extent, outweigh the protection for privacy. Curtis, for example, maintained that ‘[in] general terms, the acts and practices of the Court, in respect of personal information collected either directly or indirectly in the course of the exercise of the Court’s judicial functions, are exempt from coverage under the IPPs’, 56 while NPPs does not cover all private sectors. Regarding DLPP, it is observed that:

the doctrine ....only extends to the protection of confidential information [and] .... it is likely that communication of information via unprotected e-mail, or otherwise unprotected information, would be inconsistent with any later claim that the information was of a confidential nature. 57

Nevertheless, there is no denying the fact these voluminous laws and principles provide a strong recognition to the growing concerns of privacy and the level of their sophistication meet the international standard for balancing the traditional approach to open court with the right to privacy. The experience also helps formulate some fundamental methods for protecting privacy in the e-court that India could think about. These can be described as follows; and for which the author is not claiming any originality.

56 Ibid.
57 Ibid.
4.1. Enacting Specific Legislation on E-court

As referred to earlier that the IT Act 2000 of India focuses on privacy from a very generalized perspective and therefore privacy issues in terms of e-court are not covered by the Act. A specific legislation on e-court addressing its all aspects ranging from filing to the overall management, the rights and obligations of all participants in the judicial proceedings should be enacted. The law will provide ways to deal with confidential information while set a uniform standard for accommodating both the open court principles and privacy rights.

4.2. Developing Privacy Guidelines

An independent body with appropriate authority and expertise should be established under the e-court law which prime responsibility would be to monitor the compliance of the law and issue privacy guidelines for the court. The guidelines may contain some common principles, as in Australia, such as what information the court should collect and for what purposes, how that can be used, what circumstances and to whom that could be disclosed and what are possible security measures that the court should employ in its website to protect the information. Pursuant thereto, all state and federal courts must comply with these guidelines in conducting e-trials and in developing their databases. By adhering to the guidelines the court will promote a good culture that encourage other public and private agencies too to follow in regulating their electronic communications.

4.3. Promoting a Sophisticated Access Policy

Based on the law and guidelines a strong access policy with adequate IT support and restricted search programs should be adopted in India in dealing with e-court records. By developing specific search tools this policy must seek to prevent publication of sensitive
and other information that is irrelevant to open court consideration but has devastating consequences for litigants. In this regard, a Canadian Report recommends a search tool which is designed in a manner that ‘limits the technical possibility of aggregation of information and secondary uses that are not related to the rationale for open access to court records. In particular, the policy will obligate courts to inform litigants about the objectives of the policy and what information they are making public. This knowledge will enable litigants to assess the level of risk inherent in electronic filing and to make their own choices regarding disclosure. The policy can also make rooms for a selective publication of court records so that family related offences and other sensitive information could be excluded from the list of publication. The Family Court of New South Wales, for example, only publishes selected and edited decisions through the electronic services.

4.4, Introducing Categorical Approach

This approach concentrates on the types and nature of data and the level of protection these may require to be secured implying that all court records depending on their nature should be stored separately in different levels and require separate regulations. Records containing sensitive information including criminal and medical history should be subject to a strict regulation for access than others, which may also be suppressed from publication by the operation of law. Some of the suggestive measures may overlap with the access policy, but still the specific focus on these confidential issues could ensure

59 Model Policy n 25.
60 Cannon 2001at 105.
61 A Stanfield, Cyber courts: using the Internet to assist court processes cat.mist.fr/?aModel=afficheN&cpsId=2309045.
62 Kitajima 2000 n 8 at 571; Cannon 2004.
more vigilant and effective application of e-technology and thereby promote safeguard
against privacy assault. Special focus should also be placed on those officials who are
responsible for preparing and publishing court records online.\textsuperscript{63} By knowing this method
they will be aware of the extent to which information should not be made public, and that
will minimize the risk of abuse.\textsuperscript{64}

4.5, Advancing Self regulation and Good Practice

The statutory and administrative obligations apart, each court should develop some forms
of voluntary mechanism such as training programs and self-regulation to sustain a good
culture for privacy practice. These methods have been proven effective worldwide in
attaining desired goals and in promoting a culture of compliance. The self-imposed code
appears to persuade people more conveniently to do the needful with more care and
diligence. A regular training program reflecting international standards should include
various topics relevant to practitioners and client relationship such as the duty of care, the
test of due diligence, professional standards for maintaining confidentiality and so on.
Frequent seminars, symposium to that end, and proper dissemination of the materials
among all participants in the court proceedings may also produce encouraging results for
all regardless of judicial and non-judicial.

5, Conclusion

The electronic technology has generated a ‘new era of accessibility and publicity’ of
court records leading to rethinking of possible dangers that the society in large may have
to encounter with heavy cost. The enthusiastic e-court vision while suits the current
necessities, it has a price with ‘borderless nature’ and convenience of the Internet that

\textsuperscript{63} Model Policy n 25.
\textsuperscript{64} Cannon 2001 at 105; Kitajima 2000 n 8 at 572.
necessitate to curtail open access to court records by a statutory mandate.\textsuperscript{65} The failure to ensure a careful application of this mandate may produce unthinkable and serious hazards which can even crash the vehicle of justice.\textsuperscript{66} Our goal to establish a logistic balance between open court and individual privacy right will not be achieved should we fail to fix a tight regulated route where the co-existence of both would be safe and secured. The paper thus concludes by borrowing a prophetic comment from Stanfield, ‘our’ goal then is simple, albeit difficult: as we begin a road trip of unprecedented dimensions we must not only map the roadway but also create the very traffic rules and customs needed as we cruise down the speeding Information Superhighway.’ \textsuperscript{67}

\textsuperscript{65} Kitajima 2000 n 8 at 583.
\textsuperscript{66} Stanfield n 61.
\textsuperscript{67} Ibid.