Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 1 / ISSUE 3 / DECEMBER 2006 / 58 - 67

This paper is Available online at
www.jtaer.com

Information Protection Management Structures in Australian E-courts

Lauren May[1] and Mark Burdon[2]

[1] Information Security Institute, Queensland University of Technology, l.may @qut.edu.au
[2] Information Security Institute, Queensland University of Technology, m.burdon @qut.edu.au

Received 28 November 2005; received in revised form 08 May 2006; accepted 20 July 2006

Abstract

This issues paper is concerned with ensuring the integrity of Australia's e-court processes through the development of information protection standards and protocols. The integrity of the court process is important to the national interest because businesses and citizens depend on the certainty of court decisions, naturally assuming that their information and privacy is protected. This paper is a catalyst for future research leading to the creation of an information protection framework, including policies and standards enabling courts to define the use of courtroom technologies, thus ensuring that their design and application is grounded within established information protection principles. Without substantiation of the quality of technological structures and processes used by e-courts, the system of certainty upon which the courts and law are based has the potential to become inherently uncertain.

Key words: e-courts, courtroom technologies, security framework, security management, information standards.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 1 / ISSUE 3 / DECEMBER 2006 / 58 - 67

This paper is Available online at
www.jtaer.com

1 Introduction

Contemporary information technologies (IT) constitute infrastructures upon which our societies now rely. Our court system is no exception even though the introduction of new technology into the mainstream has been at a slower, more cautious rate than other governmental and industrial sectors. Interactions with courts are still predominantly paper-driven but the development of electronic courts (e-courts) and concomitant electronic processes are experiencing a shift from traditional silo-based working structures to new business processes and systems. Initially, IT was solely used as an automation and presentation tool. Today's information communication technologies (ICT), however, allow for systems which are more sophisticated and modularised with potential for broader and deeper capacity.

This background paper is designed to highlight the importance of formal information security management structures in Australia's e-court system. This paper contends that a comprehensive information security perspective is required to augment wider environmental structural implementation, thus ensuring the secure protection of sensitive information at the infrastructure level. Accordingly, formalised industry standards and best-practice guidelines should be developed regarding the use of e-courts and electronic court processes.

2 Structure of Research Project

2.1 Approach

The legal profession is steeped in tradition and precedence. Legal practices are inherently manual and paper-based and have been developed over centuries. Some court systems have embraced technological development whilst others have been less enthusiastic to move away from traditional working practices. This ad hoc approach has resulted in an uneven use of ICTs leading to interoperability and compatibility issues. In an attempt to concentrate on a common approach for a common end goal, this paper advocates the formalisation of industry standards and best-practice guidelines. These must, of necessity, complement current legal practice structures and reflect established information protection principles.

As this is applied research, an integrated framework is proposed that allows court practitioners to incorporate their best-practice techniques into a comprehensive information infrastructure in a structured and cohesive manner. The research project is therefore cross-disciplinary to enable the researchers to undertake a comprehensive and rigorous assessment of the legal and technological implications of information security practices in the e-court domain. The cross-disciplinary approach is necessary to gain a better understanding of the interaction between law and information security issues inherent in the use of electronic documentation in court systems. Court rules and procedures are likely to impact upon the classification and the use of certain court documents whilst the use of new electronic court documents challenge the assumptions of paper-based court rules and systems. The combination of law and information security disciplines is essential to understanding the complex interplay of legal rules and technological court systems.

2.2 Methodology

The research is qualitative by nature and a study of the legal profession necessarily lends itself towards an examination of current practices. The research project fits very broadly into the qualitative research genre because it focuses on individual lived experience illustrated by mainly phenomenological approaches, as described by Marshall and Rossman [12]. This methodological approach enables a study of both the Australian current practice experiences (phenomena) and investigations of international jurisdictions' current and past practices (phenomena) which lend them to extrapolation in the target Australian environment. In this manner the research project also takes a lessons-learned approach from the legal-practice aspects of information processing. By that, we mean that world-wide best practice will be investigated, particularly in the USA and then applied to the Australian situation to assess whether anything can be gained from experience in other international jurisdictions.

Marshall and Rossman [12] define the following characteristics of qualitative research: it takes place in the natural world; it uses multiple methods that are interactive and humanistic; it is emergent rather than tightly prefigured; and it is fundamentally interpretive. Our research takes place in the real world and we use a combination of a survey instrument, observation and peer discussion to integrate our results. The conceptual model is emergent stemming from practice development over time, and the research is interpretive in that we focus on current and past lived experience within the legal profession and extrapolate towards end goals.

Marshall and Rossman [12] also indicate the need for a good understanding of the complex interactions, tacit processes and often-hidden beliefs and values which highlight the potential of the study to improve on current practices. In the essentially manual-based legal profession commonly held perceptions, norms and customs, as well as implicit standards, proliferate. A systematic approach and well-conceived methodology for this research assists with identification and interpretation of many of these phenomena, which in turn contributes towards the significance of this research.

Firstly, it is envisaged that a wide-ranging legal and technical literature review will be undertaken to ascertain existing Australian and international court rules, information security practices and technologies currently in use. Issues of importance will also be identified. Secondly, it is proposed that a qualitative survey instrument be developed, probably based on telephone and face to face, semi-structured interviews, of Australian court practitioners to obtain data on the current situation regarding information security practices in e-courts, ICT usage in e-courts and issues of importance to Australian court practitioners. Thirdly, a case study of a court proceeding using ICTs will be conducted to observe the legal and technical practices currently in operation particularly from an information protection management perspective. The form of qualitative data analysis recommended by Miles and Huberman [15] (observation of current and past practices) will be employed. Once data on world-wide best practice and the current Australian situation has been collated, a conceptual framework will be designed to formulate information security standards specific to Australian e-courts.

2.3 Framework

Standardization in this context entails taking a holistic approach to the e-court business functions being fulfilled that involves both the technologies and the technology users. Accordingly, the research project aims to develop a conceptual "set of standards" for Australian e-courts that are linked together in a hierarchical (or triangular) structure, as detailed in Figure 1. Relevant issues are addressed from a high conceptual design and upper management level (at the peak or vertex of the hierarchy), through the medium application management and implementation level and onto the lower best-practice guideline checklist operational level (at the broader baseline of the hierarchy).

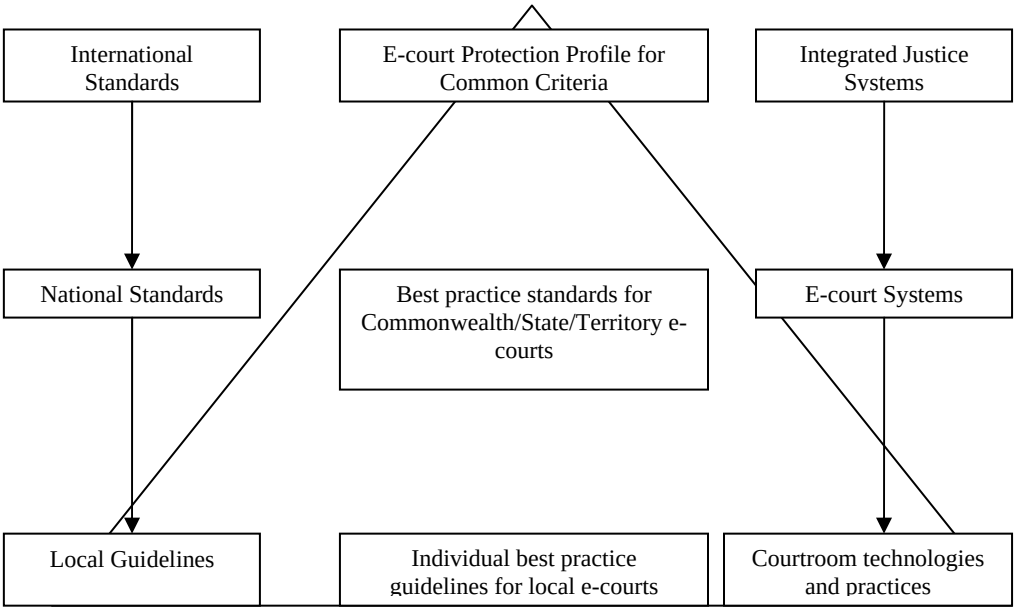

Figure 1: Set of Standards Triangular Concept

2.4 Preliminary Research Questions

The preliminary purpose of the research is to undertake an exploratory analysis of current practices in Australian e-courts and existing or past practices in international e-courts (initially USA). In order to determine and develop strategies for improving technological processes in e-court environments, one first needs to gain an understanding of current phenomena within practice environments to identify relevant issues, barriers and enablers in pursuit of the end goal. As such, we developed three preliminary research questions to help our understanding or the current situation and to provide a thematic structure for the literature review.

1. Has previous research been conducted into information protection practices in e-courts?
2. Are information protection standards required for e-courts?
3. Are there any information protection standards currently in place?

2.5 Literature Review

The research project started with an extensive literature review that took a thematic approach to potential topics of interest. The literature review covered four separate but related topics, namely: e-courts, electronic litigation (e-litigation), information technology usage by the legal profession and information security issues in all three areas. It

was important to gain some understanding of the use of ICTs in law firms and the legal profession to gain a comprehensive understanding of current technological and information security practices. Moreover, it was as equally important to gain some form of understanding as to how information security concerns were currently resolved within the e-court and legal profession domains.

Key search terms for the four topics were developed and over 1,800 references were retrieved. A thematic classification structure was developed to categorize references into each topic. The vast majorities of references is American and are from profession-related journals that rely heavily on description rather than analysis.

2.6 Research Definitions

One of the first aims to resolve in this project, and indeed, law and information security cross-disciplinary research in general, is learning, accepting and defining a common and agreeable language to frame research questions. The disciplines of law and information security bring with them their own languages and cultures. A starting point has been to establish an agreed vocabulary of terms for words that have different meanings to both disciplines. For example, when a technologist talks of 'integrity' they mean definitively that a certain piece of information has not been changed whether accidentally or on purpose. A legal professional or law academic, however, refers in the abstract to notions of ethical behaviour.

Language issues are readily visible when court practitioners (solicitors, barristers and judges) are asked about "information security". Preliminary discussions have revealed that the term appears to carry technological and/or negative connotations with which court practitioners do not associate as being within their realm of interest. This reflects the hierarchical nature that pervades legal cultures which clearly delineates between senior/junior staff and practitioner/support personnel. Hence "information security" appears to have an isolating effect indicating that it is viewed by court practitioners as a solely technological issue to be resolved by IT support staff. Alternatively, "information protection" appears much more acceptable to court practitioners possibly because it is an all-inclusive term that reinforces their cultural notions of ethics and confidentiality, with which they do associate. Experience indicates that successful information security applications include an environment of staff participation. As a consequence, in the context of this paper and the ongoing research, "information protection" is synonymous with "information security".

Different definitions of an e-court currently exist. Commonly, an e-court refers to the concept of a court that has the facilities to operate a "paperless trial" [18], [10]. The definition envisages a physical court which uses courtroom technologies during trial and pre-trial proceedings. Courtroom technology is in itself a generic expression used to describe numerous forms of technology that may or may not be collectively present in any given courtroom [8]. Courtroom technologies typically include document imaging systems, real time transcription software, case management databases, video conferencing facilities, digital video and audio recording, access to the Internet, e-mail and external intranet access.

Alternatively, the Federal Court of Australia defines an e-court as "a web-based forum which the Federal Court uses as a virtual courtroom for giving directions and other interlocutory orders on-line. When using eCourt, the Court may receive submissions and affidavit evidence and make orders as if the parties were in a normal courtroom." [5]. The Federal Court's e-court is not a physical courtroom and has limited functions as it facilitates a process for handling interlocutory matters only and does not cover all aspects of trial proceedings (though it is acknowledged that the Federal Court does foresee using an actual courtroom for certain trials involving courtroom technologies).

The Productivity Commission, in their review of government services adopt a different definition for "electronic courts" [19]. This definition refers to court systems, such as the PERIN Court in Victoria which is designed to "resolve large numbers of unpaid infringement notices in such a way as to reduce the load on the judicial and administrative resources of the hearing courts" [4]. This definition of "electronic court" refers to a fully automated IT process that automatically imposes fines on unpaid infringement notices and does not involve any trial proceedings and does not refer to an actual physical court environment.

We recognize the flexible terminology regarding e-courts. For the purposes of this research, an e-court is defined as a body with an adjudicative function that makes use of ICTs to run its proceedings. The definition refers to an actual, physical courtroom. It is broad in scale to encompass different types of courts and to include aspects of both the "paperless" and "virtual" courtrooms mentioned above. The research does not cover fully automated "electronic courts" or commissions of inquiry. The ICTs referred to are the courtroom technologies detailed above, though it should be noted that the technologies mentioned are not intended to be an exhaustive list.

3 E-courts in Australia

The literature indicates that Australia has been one of the frontrunners in the development of e-courts and courtroom technologies [9] [27]. Initial development was reactive in nature, in the sense that new courtroom technologies were implemented to meet fresh demands caused by the specific requirements of several very complex pieces of criminal and civil litigation, and also by lengthy commissions of inquiry in the early 1990s [11] [26]. For example, the Estate

Mortgages litigation in Victoria involved twelve active parties, who instructed a total of 27 counsel, which led to an estimated cost of $500 per minute to run proceedings [24]. The Wood Royal Commission into police corruption in NSW took two and a half years to conclude.

Given the large cost and the length of time complex commissions of inquiry and litigation can take, it is not surprising that courtroom technologies were implemented to increase the efficiency and the effectiveness of court proceedings. Implementation has proceeded to the extent that courtroom technologies are now standard in royal commissions [11]. Commonwealth, State and Territory courts all rely on ICT to varying degrees during their proceedings, though some jurisdictions are more advanced than others. That said, e-courts are still only used during matters of complicated and large-scale litigation, such as the Channel 7 v Foxtel case currently being heard in the Federal Court.

Currently, there are no statistics within or across jurisdictions to record how many electronic trials are conducted in e-courts. Anecdotal evidence suggests that usage is still patchy and most trials are still predominantly paper-based. However, there is little doubt that all jurisdictions see e-courts as the way forward as the Commonwealth and all States/Territories have at least one e-court and some court systems are committed to further enhancing their information technology capabilities. Moreover, some Australia jurisdictions are developing case law in which the use of court technologies will be imposed on litigants if the court believes that it will be more efficient and effective to conduct an electronic trial [6]. Finally, a range of informal standards, in the guise of court Practice Notes, has been created to encourage and manage the use of electronic data and scanned documents during pre-trial and electronic trial hearings [17].

It is therefore possible to view the development of e-courts in Australia as a suite of courtroom technology tools, used for different functions, but coming together in a common environment, to form the foundation of a technological e-court framework. This framework has been based on an ad hoc, incremental development as technologies devised for one matter or court have been further adapted for use in subsequent cases.

3.1 Integrated E-court Structures

The first phase of technological development within e-courts was the application of the courtroom technologies themselves. In a sense, the initial impetus was on building more sophisticated automation and presentation tools. The succeeding years saw a shift in focus from the tools themselves to the technological structures that support those tools. The Federal Court of Australia's e-court Integration Project [23] encapsulates thinking on e-court process realignment. Business process alignment is at the heart of the project by looking at how technology can function across a range of different courts within the same technological environment and using the same business processes. The realignment to a "User Centric Model" proposes seamless access to all information required in relation to any court file [23]. State examples of developing technological structures can be seen in Victoria [26], Western Australia [28] and Queensland [22]. In Victoria, for example, the Courts Strategic Direction Statement provides for structural reform of the court service with the aim of creating "coherent, integrated system-wide approach to long term strategic planning". The approach is underpinned by a new information technology platform, Integrated Courts Management System, which would provide a means for the public to interact with the courts and links the Victorian court structure, via several unified systems, including a cross jurisdictional approach to the use of court technologies [3].

Court systems are moving to a position that other government sectors and industries reached during the last decade, namely, implementing ICT to improve efficiency and effectiveness by replacing traditional manual, paper-based systems. In that sense, it is possible to view the development of e-courts within a wider e-government context. The court systems are an essential arm of government and the governance of society. ICT developments within courts are very much focused upon increasing cost effectiveness but they also have a key role to play in enhancing access to court services and information for users, particularly via the Internet. These are the key characteristics of e-government initiatives yet it is interesting to note that the development of e-courts is seldom mentioned within an e-government context.

Perhaps a reason for this is that courts have been relatively late adopters of ICT. It is hoped that further research will provide a clearer indication of why that has been the case. The researchers' preliminary hypotheses suggest that cultural issues within the legal profession may have been a factor. The practice of Common Law justice is conservative as it is dependent upon evolutionary principles through the application of centuries' old legal precedent. The implementation of ICT is a revolutionary process as the act of technological integration slices through many traditional working structures and practices. Moreover, there are multiple senior executives within court systems (judges, court administrators, senior barristers, and senior solicitors) and the impetus for change may well be fractured and disparate. Therefore, the driver for ICT implementation may not exist at a senior level and may even take the form of a conscious or sub-conscious resistance to change. It should not be underestimated how attached senior judges and lawyers are to the paper-based world.

3.2 Information Protection Issues

Courts are advancing towards widespread acceptance of ICTs as integral components of many legal structures and processes. As ICT usage comes of age, these new legal structures and processes will become part of the wider information infrastructures which define modern societies– our critical information infrastructures. Critical infrastructures are defined by the Australian Government as those facilities which, if compromised for an extended period, would significantly impact upon the well-being of the nation. Critical infrastructure protection is concerned with ensuring the integrity of the nation's critical infrastructures. This is achieved through a number of approaches, one of which is ensuring the integrity of the court process which directly affects integrity of law enforcement and crime prevention [25].

The integrity of the court process is akin to a critical information infrastructure and it is important to the national interest because litigants depend on the certainty of court decisions. An intrinsic reliance is placed on courts and law firms to protect their clients' information and privacy during the litigation process. This reliance has perhaps not been fully translated to e-courts. A potentially disturbing trend within court practitioners is the inherent assumption or reliance on third party providers that courtroom technologies are somehow automatically 100% "secure". "Other industry" experience shows that industry-level security services are most successfully achieved through a holistic approach - through the creation of an information protection framework, including policies and standards, designed specifically for the required environment.

In his 2003 address to the "Courts for the 21st Century: Public Access, Privacy and Security" conference at the QUT School of Law, Caelli addressed some prospective pitfalls by highlighting inherent technological security issues with respect to a recently published e-court proposal in the Sydney Morning Herald newspaper. The presentation focused on several fundamental information protection mechanisms and widely-accepted design misconceptions including connectivity, end-to-end secure channels, archiving, time/date stamping and signing of documentation. Discussion of these issues focused on a "lessons learned in other industries" perspective and the paper concluded with a brief overview of the use of standards to ensure public confidence in the courts system [2].

Caelli highlighted that there is scope for potential information protection problems within Australian e-courts. The degree of instability and potential insecurity has thus far been small because the adoption of court technologies has been relatively limited. Our preliminary findings indicate that court systems are moving to expand the use of courtroom technologies and to re-align existing processes around ICTs. Consequently, the scope of the potential problem will increase commensurate with the implementation of these new technological structures and processes that have not been conclusively tested within an information security context.

4 Research Findings

This section details findings based on the research undertaken from the literature review.

4.1 Lack of Formal Research

There is a lack of formal research into information protection issues in Australian e-courts. Although the more generic information security discipline is well-represented in public domain literature, a review of the literature revealed that Caelli's paper was the only specific reference to information protection issues in Australian e-courts. Another relevant paper that should be noted is that of The Law Society of New South Wales which published an issues paper looking at information security concerns regarding online transactions with particular attention on authentication [7]. The Law Society paper is limited in focus to the extent that it only covered the processes involved in electronic filing of documents from predominantly a practitioner's point of view whereas Caelli's paper provided a critical approach to structural e-court information protection questions.

A minimal number of international references were also retrieved. Most references were American and this is not entirely surprising given that e-courts are more established in the USA than Australia. In general, individual court practitioners within their respective legal professions raised issues indicating that the professions are still wrestling with the development of new ICTs.

4.2 American E-courts Are More Advanced

The adoption of courtroom technologies and the formal use of e-courts are more advanced in the USA than Australia. The usual path to ICT acceptance within any given industry is: first, a period of individual trial-and-error ad hoc approaches, generally aimed at replacing manual processes; second, realisation of the need for interoperability, away from numerous information "silos" towards a more manageable system; third, recognition of the requirement for standardisation, in line with alternative good business practices; and, finally, acceptance of the formalisation of the management of information into the normal business management structure. As a general rule, the more advanced is the industry along this path, the more mature is the contribution of the technology to the industry and the more accepting is society towards that industry's credibility and authority.

In an ICT-driven world, court practitioners are faced with the same issues as any other industry. American court systems are currently at the second stage and fast approaching the third: the recognition that interoperability and standardisation are paramount. For example, the National Center for State Courts (NCSC) is a truly national organization whose mission is to "improve the administration of justice through leadership and service to state courts, and courts around the world" [16]. The NCSC runs an annual e-courts conference and at the 2004 NCSC conference, participating court practitioners raised a number of information protection issues that could be resolved by information security approaches which have been tried and tested in other industry information infrastructures. The Sedona Conference is a research and educational institute dedicated to the advanced study of law and policy including complex litigation [20]. The organisation has developed a series of best practice guidelines for managing electronic records that would be directly relevant to Australian e-courts [21]. The American Bar Association's Information Security Committee (ABA ISC) also explores legal and technical aspects of information security from the perspective of the legal profession.

It would appear that Australian court systems are still somewhere between the first and second stages – individual trial and error, ad hoc approaches combined with the realisation that greater interoperability and information management are required.

4.3 An American Information Protection Incident

The literature review did reveal one information protection incident that could be relevant to Australian e-courts. Messing and Teppler [14] highlighted concerns regarding the transparency and reliability challenges facing e-court processes and provided a real-life example of how court employees in Riverside, California illegally altered criminal records to show that charges had been dismissed against five defendants when in fact they had not. The employees accessed court records by remotely dialling into the court's case management database using passwords obtained whilst acting as consultants to the local police force. The authors concluded that "no longer can we presume courts have authoritative record of electronic filings unless court computer security is technically assured".

Messing and Teppler [14] also discussed trust issues arising where the integrity of judicial orders, for example, may come into question. "Integrity" in this context refers to the property that the judicial orders have not, either accidentally or on purpose, been altered during communication and storage after the order has been made. The contribution of this paper is in raising awareness that information protection is needed for e-court applications. Other presentations at the NCSC 2004 E-courts Conference pointed out quite realistic scenarios of information system "glitches" that have the potential to undermine the authority of the judicial process.

4.4 No Current Australian E-court Information Protection Standards

There are no published information protection standards for Australian e-courts. Instead different Australian legal jurisdictions have developed Practice Notes that focus on scanned electronic document and data exchange and do not feature a broad information protection outlook. Moreover, the Practice Notes have been developed at the behest of the courts, in conjunction with the providers of courtroom technologies. As such, the directions are narrow in their focus and are very much based on the court's and suppliers requirements, in an attempt, to ensure the most efficient and effective way of conducting data and document transfer within an electronic trial.

In contrast, the NCSC has attempted to develop and implement e-court information protection standards. These standards cover a range of issues including the integrity of electronic records, the accurate recording of submission times of electronic documents, the identity of the filer of documentation and the preservation of integrity in transmitted documents and data. Australian legal jurisdictions have thus far not attempted to address this issue [13].

4.5 Summary of Research Findings

The table 1 below summarizes our research findings.

Research Question	Preliminary Finding
Has previous research been conducted into information protection practices in e-courts?	Virtually no formal research has been conducted into information security issues in the legal profession and the court system. Moreover, it would appear that there has been no research into information security issues or information technology usage within Australian court systems.
Are information protection standards required for e-courts?	Australian court systems are increasingly using ICTs to fulfill their core business functions and to expand upon current technological systems. Caelli's paper on information protection issues in e-courts highlights potential fundamental design insecurities which are predicated on notions that the technologies provided are automatically %100 secure. Accordingly, information protection management structures are required

	to ensure the safe expansion of ICT systems. In the USA, Messing and Teppler provided a real life example of an information protection incident involving a USA court system. Whilst the incident did not involve an e-court *per se*, the same principles regarding the lack of information protection management practices are still applicable.
Are there any information protection standards currently in place?	There are no published information protection standards specific for Australian e-courts. Instead, different Australian jurisdictions have developed Practice Notes that have a limited application that focuses on the management of information. In the USA, however, the NCSC has developed a range of information protection standards specifically for e-courts.

Table 1: Summary of research findings

5 Future Research

The focus of this research is to develop information protection standards and management structures to ensure maximum worth of ICT usage and to maintain the confidence that society demands of our court systems. This involves identifying usage properties and matching these with well-understood techniques leading to the creation of an information protection framework to certify that e-court applications are grounded within firm information security principles.

Standardization involves more than just agreeing on a set of hardware and software that all parties are content to use. In its generic sense, the terminology "standard" has many loosely-defined meanings. Formal information protection standards provide for the quality service of technology by applying security techniques and mechanisms to achieve fundamental goals and services. Typically information protection goals include services such as confidentiality of data, integrity of information, authentication of data source, non-repudiation and availability of data. Protection mechanisms are the managerial and technological methods, protocols and primitives which are employed in order to achieve the desired information goals.

An essential foundation for this approach is that of information protection whose main goal is to ensure the quality of information. There is an assumption that these new court information infrastructures will automatically be able to protect our information, but this is not inherently so. With motor vehicles, a unit designed developed and created with safety in mind from the outset will, in general, produce a vehicle with superior safety features. Similarly, the incorporation of information protection within the design development and creation of e-court information infrastructures at an intrinsic level will, in general, produce information management of the highest quality.

The team of researchers from QUT includes law and information security academics as well as an industry partner organisation. The team's intention is to develop this project through the Australian Research Council (ARC) system.

6 Conclusion

Messing and Teppler provided a realistic and foreseeable example of problems when they highlighted the possibility of accidental or deliberate alteration of judicial decisions with no recourse to audit trails or management systems to validate integrity. It is these issues of trust that could cause significant damage to the reputation of the court and the judicial process because our society places so much confidence in the belief that our personal information will be kept secure when we interact with the courts and the legal profession. At the same time, our society consents to follow the rulings of the court whether they are thought to be right or wrong. The whole system is based on trust and confidence. For this reason alone, it is vital that courts have total confidence in the integrity of their new technological systems for society to maintain its trust in court decisions.

Currently, the wisdom of ICT usage within contemporary court and legal environments is still a matter of debate because legal processes are still largely paper-based. This issues paper has established that, regardless of philosophical attitudes, ICT usage is occurring today within the court and legal environment and is showing signs of increasing. Without substantiation of the quality of technological structures and processes used by e-courts, the system of certainty upon which the courts and law are based has the potential to become inherently uncertain. Any degree of instability could weaken trust and confidence in the court system at a local, national and international level. This in turn could have direct consequences on national security because the maintenance of law and order is partly dependent upon the degree of certainty our society demands from the courts.

There is a need for standardisation of ICT applications in the e-courts environment based upon an information protection foundation to maintain confidence in new technological court processes. We conclude that formalised

industry standards and best-practice guidelines should be developed to ensure the integrity of Australia's e-court processes.

References

[1] American Bar Association. (2006, July.) Section of Science & Technology: Information Security [Online]. Available: http://www.abanet.org/dch/committee.cfm?com=ST230002.
[2] W. Caelli. (2006, July). E-Security, Information management and Archiving in the Public Sector [Online]. Available: http://www.law.qut.edu.au/files/ecourts-qut-061103.pdf.
[3] Department of Justice, Victoria. (2006, July.) Integrated Courts Management System [Online]. Available: http://www.justice.vic.gov.au/CA2569020010922A/page/Courts+and+Tribunals-Integrated+Courts+Management +System +- +ICMS? OpenDocument& 1=0-Courts+ and+Tribunals~&2=0-Integrated+Courts+Managment+System+-+ICMS~&3=~.
[4] Department of Justice, Victoria. (2006, July). PERIN Courts. [Online]. Available: http://www.justice.vic.gov.au/CA2569020010922A/OrigDoc/~BFACF878B20014EFCA256D4F0023DF67?Open Document&1=10-Listing~&2=0-Perin+Court~&3=01-PERIN+Court+-+Overview~
[5] Federal Court. (2006, July.) Practice Note No 17 - Guidelines for the Use of Information Technology in Litigation in any Civil Matter [Online]. Available: http://www.law.mq.edu.au/Units/law404/E-Court%20FCA%20Practice%20Note. htm.
[6] Harris Scarfe & ORS v Ernst & Young & ORS (No 3) [2005] SASC 407; Idoport v National Australia Bank Ltd (2000) 49 NSWLR 51 and Kennedy Taylor Pty Ltd v Grocon [2002] VSC 32.
[7] S. Kay, Security and Authentication Requirements in the Court Process: part 1: Current Security Practices and Requirements and Survey of Courts' Approaches to Online Security in Australia and the US, Internet Law Bulletin, vol. 4, pp. 5-13, 2004.
[8] F. I. Lederer, Technology-Augmented Courtrooms: Progress Amid a Few Complications, or the Problematic Interrelationship Between Court and Counsel, New York University Annual Survey of American Law, vol. 60, pp. 675-709, 2005.
[9] F. I. Lederer, What Have We Wrought?, William and Mary Bill of Rights Journal, vol. 12, pp 637-648, 2004.
[10] F. I. Lederer, The Road to the Virtual Courtroom? A Consideration of Today's--and Tomorrow's--High-Technology Courtrooms, South Carolina Law Review, vol. 50, pp. 799-844, 1999.
[11] R. Macdonald and A. Wallace, Review of the Extent of Courtroom Technology in Australia, William and Mary Bill of Rights Journal, vol. 12, pp. 649-659, 2004.
[12] C. Marshall and G. Rossman, Designing Qualitative Research. London: Sage Publications, 1999.
[13] L. May and M. Burdon. Ensuring the integrity of Australia's ecourt process. Recent advances in security technology: Proceedings of the 2006 RNSA Security Technology Conference, Canberra, Australian Homeland Security Research Centre, pp. 259-273, 2006.
[14] J. Messing and S. Teppler. (2006, July) Preventing a Pandemic of Judicial Identity Theft: Transparency and Reliability Challenges Facing Ecourt Processes and Output Today [Online]. Available: http://www.e-courts.org/presentations/messing.pdf.
[15] M.B. Miles and A.M. Huberman, Qualitative Research. London: Sage Publications, 1994.
[16] National Center for State Courts. (2006, July). NCSC Mission Statement. [Online]. Available: http://www.ncsconline.org/.
[17] New South Wales: Practice Note No 127 Use of Technology in Civil Litigation, with effect from 1.3.2004; NT: Practice Direction No 2 of 2002, Guidelines for the Use of Technology in any Civil Matter, published 13.2.2002, Vic: Practice Note, No 1 of 2002 Guidelines for the Use of Technology in any Civil Matter, published on 29.4.2002; Federal Court: Practice Note 17 Guidelines for the Use of Technology in Litigation in any Civil Matter, published April 2000.
[18] R.D Nicholson, The Paperless Court? Technology and the Courts in the Region. Journal of Judicial Administration, vol. 12, pp. 63-84, 2002.
[19] Productivity Commission. (2006, July). Report on Government Service [Online]. Available: http://www.pc.gov.au/gsp/reports/rogs/2005/chapter06.pdf
[20] Sedona Conference. (2006, July). The Sedona Conferences [Online]. Available: http://www.thesedonaconference.org/
[21] Sedona Conference Working Party. (2006, July). The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age [Online]. Available: http://www.thesedonaconference.org/content/miscFiles/TSG9_05.pdf
[22] J. Sherman and I. Sims. (2006, July) Supreme & District Courts: IT Action Plan – 2002 [Online]. Available: http://www.courts.qld.gov.au/publications/SJA/IT%20Action%20Plan_small.pdf.
[23] J. Sherman and A. Stanfield. (2006, July) Federal Court of Australia: eCourt Integration Project - Final Report [Online]. Available: http://www.aph.gov.au/SEnate/committee/legcon_ctte/estimates/bud_0405/ags/155_att.pdf.
[24] T. Smith. (2006, July) AIJA Annual Conference - The Estate Mortgage Court System. [Online]. Available: http://www.aija.org.au/conference98/papers/estate/index.htm
[25] TISN. (2006, July) About Critical Infrastructure Protection [Online]. Available: http://www.cript.gov.au/agd/www/TISNhome.nsf
[26] Victorian Law Reform Commission. (2006, July), Technology and the Law [Online]. Available: http://www.egov.vic.gov.au/pdfs/techlaw.pdf.

[27] A. Wallace, The Challenge of Information Technology in Australian Courts, Journal of Judicial Administration, vol. 9, pp. 8-36, 1999.
[28] M. Warren, Modernising Justice: IT and the Supreme Court, Law Institute Journal, vol. 79, pp 44-5, 2005.