ARTICLE:

BUSINESSES' PERCEPTION OF ELECTRONIC SIGNATURES: AN AUSTRALIAN STUDY

By **Dr Aashish Srivastava**

Introduction

The advent of the internet has transformed the world of commerce. Electronic commerce allows businesses to buy and sell in global markets that are no longer bound by geography or time. Increasingly, governments, businesses and consumers are using information technology and the internet to exchange information, produce, market, buy, sell and even deliver products and services to places virtually unreachable before. Electronic signatures,[1] in particular digital signatures,[2] have been established with the objective to authenticate and facilitate commercial transactions in the electronic environment.

Several initiatives have been implemented over the last decade in order to provide legal recognition to electronic signatures. At a global level, the United Nations Commission on International Trade Law (UNCITRAL) has provided model laws that offer a legislative guide to countries on the framing of their national electronic signature legislation.[3] At a regional level, the Electronic Signature Directive has been enacted by the European Union (EU) in an attempt to ensure consistency and legal validity of electronic signatures across member states.[4] In addition to legislation on an international and regional level, over ninety individual countries have also legislated for the use of electronic signatures. Typically, legislation has taken one of three types of approaches: a minimalist or technology-neutral approach where any technology can be used as an electronic signature provided it satisfies the legal function of a signature;[5] a digital signature or technology-specific approach[6] that recognises the primary use of digital signatures generally to the exclusion of other forms of electronic signature; and a dual approach that provides an evidentiary presumption in favour of validity of an electronic signature if the parties use specific technologies, in particular, digital signatures issued by recognised certification authorities.[7]

In Australia, a technology-neutral legislation was enacted in 1999, the Electronic Transactions Act 1999 (Cth) (ETA).[8] Based on this Commonwealth legislation, States and Territories have enacted similar electronic signature and transaction legislation.[9] The provisions of

[1] *One definition of 'electronic signature' is provided by article 2(a) of the UNCITRAL Model Law on Electronic Signatures 2001 art 2(a), 'as data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message.'*

[2] *A digital signature is a type of electronic signature, and is described in paragraph 36 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001) as 'created and verified by using cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible form and back into the original form'.*

[3] *See UNCITRAL Model Law on Electronic Commerce 1996 and Model Law on Electronic Signatures 2001.*

[4] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19.01.2000, p.12.*

[5] *Most common law countries have adopted the minimalist approach towards legislation. These include the US, the United Kingdom, Canada and New Zealand.*

[6] *The technology-specific approach has also been referred as a prescriptive approach in the literature.*

[7] *The EU Electronic Signatures Directive is a good example of a dual approach. The legislation in China and Singapore are also considered as a dual approach. See Electronic Transactions Act 2004 (China) (for a translation and introduction into English of the Chinese Act, see Minyan Wang and Minju Wang, Translation and Introduction to the Electronic Signatures Law of China, Digital Evidence and Electronic Signature Law Review 2 (2005) 79 – 85, and Electronic Transactions Act 1998 (Singapore).*

[8] *Electronic Transactions Act 1999 (Cth).*

[9] *The state level Acts are: Electronic Transactions Act 2000 (NSW); Electronic Transactions Act 2000 (SA); Electronic Transactions Act 2000 (Tas); Electronic Transactions Act 2000 (ACT); Electronic Transactions Act 2003 (WA); Electronic Transactions (Victoria) Act 2000 (Vic); Electronic Transactions (Queensland) Act 2000 (Qld); Electronic Transactions (Northern Territory) Act 2000 (NT). Note that since the State legislation is essentially the same as the Electronic Transactions Act 1999 (Cth), the discussion in this article is confined to the provisions of the latter legislation.*

' The reluctant take-up of electronic signature tools is slowing down the growth of trade in goods and services via the internet,' asserted a press release, without any evidence.

the ETA are based on the Model Law on Electronic Commerce 1996 (MLEC) which is the first model drafted by the UNCITRAL.

Despite the legislative initiatives at global, regional and national levels to promote the use of electronic signatures, anecdotal evidence and reports in the media indicate that there has been a very slow take-up of the digital signature technology across the world. A progress report on the EU Electronic Signature Directive in 2006 expressed concern with regards to the slow take-up of digital signatures across its twenty-five member states.[10] 'The reluctant take-up of electronic signature tools is slowing down the growth of trade in goods and services via the internet,'[11] asserted a press release, without any evidence. Other countries such as Germany and Thailand have also reported low acceptance of digital signatures in recent years.[12] Some scholars in the field have expressed concern that the culture of the failure to adopt digital signatures by individuals and businesses is hard to change.[13]

Likewise, it has been almost nine years since the ETA has been enacted in Australia, but the use of electronic signatures, particularly digital signatures, has been low.[14] Note that while the legislation was enacted to give an impetus to e-commerce at all levels, digital signatures are mostly used for government on-line services.[15] Anecdotal evidence shows that there has been a low use of digital signature technology among businesses when dealing with other businesses for contracts and commercial transactions, despite the Australian government's effort to promote it as 'a valid form of authentication for enabling and sealing e-commerce transactions'.[16]

Research questions

This led the author to consider a number of questions. Why is there a lack of acceptance of digital signatures by the business community in Australia for entering into contracts and commercial transactions with each other? What could be the likely factors to impede the use of electronic signatures, in particular, digital signature technology in a regulated environment?

The objective of this article is to briefly outline the findings of a comprehensive investigation conducted by the author as part of his doctoral thesis to identify factors that have contributed to the low acceptance of electronic signatures, in particular digital signatures, in the Australian business community. The research was an empirical study relying predominantly on the views and experiences of various groups of people from large country-wide public listed companies in Australia. A sample of 27 participants comprising of heads of the

[10] *Commission of the European Communities, Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures (Brussels, 15.3.2006, COM(2006) 120 final) http://ec.europa.eu/information_society/eeurope/i2010/docs/single_info_space/com_electronic_signatures_report_en.pdf.*

[11] *' Electronic signatures: legally recognised but cross-border take-up too slow, says Commission' (IP/06/325, Brussels, 17 March 2006) http://europa.eu/rapid/pressReleasesAction.do?reference=IP/06/325&format=PDF&aged=0&language=EN&guiLanguage=en.*

[12] *eGovernment, Take-up of electronic signatures remains low in Germany (2004) epractice.eu (no longer available); Pascale Prud' homme, and Hassana Chira-aphakul, E-Commerce in Thailand: A slow awakening, Thailand Law Forum http://thailawforum.com/articles/e-commerce.html.*

[13] *Heiko Roßnagel ' On Diffusion and Confusion-Why Electronic Signatures Have Failed' in Simone Fischer-Hübner Steven Furnell, Costas Lambrinoudakis, editors, Proceedings of the Third International Conference on Trust and Privacy in Digital Business (TrustBus 2006) 71; Jane K Winn, ' The Emperor New Clothes: The Shocking Truth about Digital Signatures and Internet Commerce' (2001) 37(2) Idaho Law Review 353; Raymond Perry, ' Digital Signatures - Security Issues And Real-World Conveyancing' (2001) 151 New Law Journal 1100. See also in the Australian context, Drugs and Crime Prevention Committee, Parliament of Victoria, Inquiry into Fraud and Electronic Commerce (2004) (180) http://www.parliament.vic.gov.au/dcpc/Reports/DCPC_FraudElectronicCommerce_05-01-2004.pdf.*

[14] *Drugs and Crime Prevention Committee, Parliament of Victoria, Inquiry into Fraud and Electronic Commerce (2004) 180 http://nla.gov.au/nla.cat-vn3093816.*

[15] *Inquiry into Fraud and Electronic Commerce (2004). The areas in which digital signatures are being promoted are: Australian Customs Service, SPEAR Project run by Land Victoria and EC (Electronic Conveyancing) system, a part of the Land Exchange Program within the Victorian Government's Department of Sustainability and Environment. The latest position is that these projects are currently running at a very small scale. Unfortunately, there is no recent information or reports that are available on these.*

[16] *National Office for the Information Economy, Government Role in B2B E-Commerce (2001) Department of Communications, Information Technology and the Arts www.archive.dcita.gov.au/2001/10/b2b_e-commerce/. The Drug and Crime Prevention Committee report states that digital signatures are used primarily with the ATO and not for other services.*

In general, participants revealed a considerable lack of understanding of the term electronic signature and the legislation governing them.

Information Technology (IT) and legal departments and senior management (SM) executives was used. A series of semi-structured interviews were conducted face-to-face or by telephone. The interviews were then transcribed and analysed by the author using the matrix-based framework analysis approach commonly used in applied policy research.[17] This article first summarises the main findings of the research. It is then followed by a critical discussion, followed by a number of recommendations for measures that may overcome the low use of electronic signatures in the business community.

The main findings

The empirical research demonstrated that there are six potential factors that are likely to have led to a low use of electronic signatures in the Australian business community. These are ignorance or lack of understanding of the technology and the law governing the technology, security concerns, legal obstacles, complexity and confusion, cost concerns, and culture and customs.

Ignorance or lack of understanding

A major finding of this research is ignorance. In general, participants revealed a considerable lack of understanding of the *term* electronic signature and the legislation governing them. Businesses appear to have a limited understanding of the various forms of electronic signature, not to mention digital signature, although they are using a particular form of electronic signature (i.e. e-mails) on a day-to-day basis. Such lack of awareness is identified as the leading reason for businesses' hesitance to use digital signatures.

Ignorance or lack of understanding of the *term* electronic signature

About a quarter of the participants admitted having never heard of the term electronic signatures. Others who were aware of the existence of this term demonstrated very limited understanding of the various forms that electronic signatures take. An electronic signature was generally believed to be a scanned image of a manuscript signature. In addition, there appeared a certain confusion between the term electronic and digital signature. The terms were used interchangeably during the interview process by a few participants.

Ignorance about the legislation

A high degree of ignorance also prevailed among businesses with regard to the legislation governing electronic signatures, in particular the ETA. More than two-thirds of the participants were not aware of the provisions of the ETA and the provisions relating to electronic signatures in Australia. Their lack of awareness emerged from comments such as: 'I don't know what the law is on using electronic signatures;'[18] 'I am not aware of any such law'.[19] On the other hand, those who were aware of the legislation mostly demonstrated a very limited knowledge of the provisions in the ETA. The following responses were noted from participants: 'I am not aware of it being a recognised form;'[20] 'I know there are viable options and there are rules around it but I do not know in great detail;'[21] 'We really haven't gone and explored the wider legal aspect of understanding or where the law sits with

[17] *Note that a five-stage framework analysis method was adopted for analysing the interview data. In stage 1 (familiarisation), the author familiarised himself with the interview transcripts and obtained an overview of the collected data. In stage 2 (identifying a thematic framework) an initial coding was conducted from the issues emerging from stage 1 to set up a thematic framework. The thematic framework at this stage was only tentative and further refining was made at subsequent stages of analysis. In stage 3 (indexing), the initial coding, or in other words the thematic framework, was applied to the data collected through the use of textual codes to identify those segments of the interview transcripts that reflected a particular theme. In stage 4 (charting) specific pieces of data corresponding to a particular theme were identified from the interview transcripts and arranged in charts, with each chart representing a specific theme. After all the indexing and charting were done in accordance with the themes, in the final stage 5 (mapping and interpretation), the key characteristics of the data collected were examined with a view to mapping and interpreting the data set as a whole. The above five steps were carried out with the help of NVivo, a software package well known for the analysis of qualitative data.*

[18] *P2_C02_Legal, Paragraph 31.*

[19] *P12_C07_SM, Paragraph 76.*

[20] *P16_C04_Legal, Paragraph 68.*

[21] *P18_C011_Legal, Paragraph 197.*

it;'[22] 'There are some legislation in 2001, the Electronic Transactions Act or something like that. That is all I remember but I am not deeply familiar with it.'[23] Businesses' lack of awareness and understanding of the legislation appeared to be largely responsible for their lack of appreciation of the different forms that an electronic signature can take. In fact, the research revealed a high level of ignorance at the level of lawyers' and legal advisors. A failure to understand the legislation appears to have potentially weakened businesses' confidence in using electronic signatures.

Security concerns

The research sought participants' views on whether security is an issue with the use of electronic signatures. In general, participants were quite concerned about the security aspect of electronic signatures. The majority of the participants believed that businesses have not embraced the idea of integrating digital signatures into their work environment for a number of security reasons. There were concerns that the technology that currently exists does not provide sufficient safeguards to users. As a result it will be impossible for digital signatures to be used as a secure form of authentication. 'It's very much the insecurity of the whole thing that is why it hasn't been widely accepted,'[24] claimed one participant. Participants were generally concerned that someone could hack into another person's computer system and maliciously use his or her digital signature without the person's knowledge.[25] '[T]he last thing you want for the other party [to the contract] to say is that 'hang on I didn't sign it, that wasn't me, I didn't do it,'[26] remarked a participant.

The security fears expressed by participants were both of technical and legal nature. From a technical standpoint, participants feared that a person could fraudulently use someone else's digital signature and pass it as his own. '[O]nce it's on the computer anyone can access it. ... it's pretty easy to get hold of it if you want to get it,' remarked a legal participant.[27] From a legal stance, participants feared that a plaintiff would not be able to satisfy the court that a forger has forged or affixed his digital signature. As remarked by one of the participants, 'when it comes down to proving, you don't know if this was actually executed by the named person.'[28]

There are three basic ways that digital signatures can be secured, through the use of passwords where a digital signature is stored on the hard disk of a computer; using portable information storage devices (PISDs); and using biometric devices. Issues were raised with all three methods of securing digital signatures.

Hard disk secured with password

The most common form of storage of a digital signature is on the hard disk of a computer.[29] A user wishing to affix his digital signature will use a key board or a mouse (or both) to activate it,[30] and the signature will then be attached to a particular data message. However, the risk is that the same command can be given by anyone else who also has access to that computer, because it is the computer that 'signs' rather than the actual owner of the digital signature. To protect from such risks, the storage of digital signatures on the hard disk of a computer can be secured through the use of a password or PIN. Participants were in general of the view that passwords can adequately protect against unauthorized and malicious access to computers. However, it was also noted that despite password security policies implemented by their organisations' IT department, staff would rarely abide by them. They would often choose passwords that would be easy to guess, or fail to change them at regular intervals as recommended. An IT participant stated:

> When you log into a system you are given a default password. My experience is that fifty percent of the people still have that password so ... anywhere down the track ... I am not sure what we really have to do ... I think if we have to move on to that ... take steps to really follow through on forcing people to change their passwords.[31]

A failure to implement precautionary measures has made digital signatures behind such passwords prone to attack. Therefore, despite the common belief among participants that the storage of a digital signature on a computer could be secured through the use of passwords, their careless attitude towards password use and management made the hard disk an unsafe option for storing electronic signatures.

[22] *P14_C09_SM, Paragraph 123.*
[23] *P21_C012_Legal, Paragraph 10.*
[24] *P8_C05_Legal, Paragraph 114.*
[25] *For example, P15_C010_Legal, Paragraph 63.*
[26] *P2_C02_Legal, Paragraph 88.*
[27] *P24_C015_Legal, Paragraph 55.*
[28] *P6_C04_Legal, Paragraph 76.*
[29] *Especially for Non-Individual digital signature certificates or Organisation digital signature certificates.*
[30] *In the case of digital signature, it is the private key that the subscriber activates to create a digital signature.*
[31] *P18_C011_Legal, Paragraph 124.*

PISDs

Digital signatures can also be stored on PISDs, such as a smart card or a Universal Standard Bus (USB) token (also known as a flash disk). A smart card is amenable to cryptographic implementation and thus enables the subscriber to sign and encrypt a document.[32] A USB token such as a flash disk, however, is not amenable to cryptographic implementation but can conveniently be plugged into the USB port which is available on most computers and laptops.

In general, participants considered the use of PISDs such as smart cards and flash disks to be unsafe. Concerns were raised by participants that PISDs could easily be lost or stolen and used for malicious purposes. '[I]f you lose a smart card who is to decide that someone else cannot read that smart card or use it,'[33] remarked a participant. However, they believed that if the PISD was secured with a password or PIN that would provide adequate security.

Biometric measurements

Apart from passwords and PISDs, another method of securing digital signatures is through the use of biometrics.[34] In this case, instead of using a password or a PISD (or both) to obtain access to his or her digital signature, a subscriber uses a biometric measurement such as fingerprint and retina scan. By using this method, although not perfect, it becomes harder for a malicious attacker to break in and use the signature than any other security mechanisms such as a password or PIN. With the exception of a few operational limitations, participants generally considered biometric measurements to be the most secure method of storing a digital signature. Their perceived views about biometric measurements were reflected in comments such as: 'that's probably a little bit more secure if it's thumb print ... that sounds fairly secure';[35] and 'I guess to crack biometric or fingers or retina or whatever, is not easily accessible to most people'.[36]

The internet and the intranet

The internet, a prerequisite for the usage of digital signature technology, was mostly believed to be insecure, although it was not considered to be a significant deterrent to the use of digital signatures. Those who found the internet insecure made remarks such as: 'I am not sure how safe the internet is ... I have concerns as to the safety of it but that is not to say that I won't use it';[37] and I don't think the internet is completely secure once you are in there it's pretty open and anything can happen'.[38]

However, some participants believed that although a digital signature uses encryption technology and can therefore secure documents traversing over the internet, it is still at risk from hackers because most office computers are connected to the internet or an intranet. According to some participants, the real risk of forgery of a digital signature does not arise primarily from the use of the internet but from fraudulent actions within an organization. As remarked one participant:

> The fraud normally is an internal fraud than transmission fraud and so I think the euphoria of people collecting thousands of cards through siphoning and data out of pay pal and things like that ... yes, a fairly strong imagination.[39]

Legal concerns

Legal concerns associated with electronic signatures were also identified as a potential factor that could contribute to its low use for contracts and commercial transactions. In particular, the lack of admissibility of electronic signatures in the court of law and complexities arising with evidentiary matters when proving authenticity of electronic signatures were raised by participants.

Admissibility of electronic signatures

A high proportion of participants, in particular legal participants, believed that electronic signatures would not be admissible in evidence. Occasionally, their legal advisors would discourage them to use electronic signatures on the grounds of their admissibility in a court of law. A legal participant remarked:

> To the end 2001 I worked on Electronic Data Interchange (EDI) type of contracts. I worked for the IT department but I have to say that apart from the EDI type stuff which never took off no-one was particularly interested in electronic signatures and the lawyer wouldn't either. The lawyer would say, 'look I don't understand all these stuff or the law won't necessarily accept it as evidence or it's too difficult. Just rely on paper or fax or something like that'.[40]

[32] *Johan Borst, Bart Preneel and Rijmen Vincent, 'Cryptography on Smart Cards' (2001) 36(4) Computer Networks 423, 423.*
[33] *P2_C02_Legal, Paragraph 64.*
[34] *Note biometric measurements can also be considered as a form of electronic signature, but are usually used to establish whether the person you are dealing with is the person entitled to the service.*
[35] *P2_C02_Legal, Paragraph 64.*
[36] *P4_C03_Legal, Paragraph 113.*
[37] *P6_C04_Legal, Paragraph 189.*
[38] *P25_C015_IT, Paragraphs 96.*
[39] *P26_C016_SM, Paragraph 57.*
[40] *P1_C01_Legal, Paragraph 61.*

Evidentiary matters

Concerns were expressed about the inconclusiveness of an electronic signature, given there is no physical document that is signed. The general view of the participants was that the law of evidence would struggle to deal with electronic signatures in the absence of original physical documents. Since there is no concept of an original digital object or a signature generated electronically,[41] the concept of primary evidence and secondary evidence cannot be applied in the context of electronic signatures. Views were expressed that courts would require the original document containing the electronic signature to identify the signer. 'The court will always look for an original. There is only one document that is an original and that is the evidence, the primary evidence,' claimed one participant.[42] 'The law very much clings to originals with a signature on it to show that they have been correctly executed between the parties,'[43] remarked another one.

Participants also feared that, unlike a manuscript signature, it was not possible to witness an electronic signature, thus adding another layer of complication. They believed that there is no provision in the law that allows the witnessing of an electronic document, in particular, an electronic signature:

> On certain contracts the execution calls provision for a witness to sign. ... they will then go to the court and testify, 'I saw that authorized officer signing this document.' With an electronic signature I find that very difficult to do.[44]

Finally, electronic signatures were subject to disapproval by participants who claimed that, unlike manuscript signatures, electronic signatures cannot undergo handwriting tests and therefore identifying the actual signatory becomes harder in case of a dispute. Thus, if a person intent on committing a fraud hacks into someone else's computer and fraudulently uses his or her electronic signature to gain an unfair advantage, it would be difficult to convince the court that neither the owner of the computer nor any authorized person used the owner's signature. In contrast, with manuscript signatures, it was asserted that a fraudulent signature can easily be identified with the help of handwriting experts. One participant offered the following comment:

> I think it would be rather difficult showing that or try to prove that there is a probability that someone else could have logged on [with electronic signatures] ... With a manuscript signature often you just need a proof. Someone can bring somebody who knows the signature or you can do handwriting tests.[45]

Complexity and confusion

The general perception among participants was that the use of electronic signatures was complex and confusing. However, these issues were raised mostly in the context of the digital signature while other forms of electronic signature were not necessarily perceived as complex to use. In particular, the digital signature technology was found to involve complicated application programs that would render it unfriendly to use; a complex setting-up process, and a stringent requirement for the recipient organisation to be equipped with a similar technology. The perceived views about the complexity and confusion were reflected in comments such as: 'I suspect that the reason for that [its non-acceptance] is that it is so complex to set up';[46] or 'the big issue is ... that it's a pain in the ass to set something up,' [47] 'You can't do it ... you can't use and communicate with that technology until you establish that the other party has that technology. I guess it adds another level of complication'.[48]

Cost

From the point of view of costs, the expenses involved in educating and training staff was identified as an important factor that could deter the use of electronic signatures. 'There is the cost of educating them as well and we are not interested in doing that';[49] the cost [of electronic signature] includes training and deployment'[50] were typical remarks made by participants.

On the other hand, the cost of obtaining digital signature certificates[51] was not considered to be a disincentive with regard to the use of the technology. Such costs were trivial for participating companies.[52] They claimed that their organisation could easily afford to use the digital signature technology. 'I wouldn't imagine that cost would be prohibitive because big companies would spend a lot more on IT systems,'[53] or 'I don't think cost would be an issue you know, if it make

[41] *Stephen Mason, Electronic Evidence: Disclosure, Discovery & Admissibility, (LexisNexis Butterworths, 2007) 2.20; 4.16-4.35.*
[42] *P1_C01_Legal, Paragraph 77.*
[43] *P18_C011_Legal, Paragraph 68.*
[44] *P6_C04_Legal, Paragraph 76.*
[45] *P18_C011_Legal, Paragraph 228.*
[46] *P1_C01_Legal, Paragraph 19.*
[47] *P1_C01_Legal, Paragraph 28.*
[48] *P22_C013_Legal, Paragraph 82.*
[49] *P5_C03_IT, Paragraph 66.*
[50] *P5_C03_IT, Paragraph 110.*
[51] *A digital signature certificate from an accredited Certification Authority such as VeriSign costs A$130-200 in Australia.*
[52] *Note that because the research confined to large Australian businesses it may be a reason that cost was not an issue. It may be an issue for small businesses.*
[53] *P2_C02_Legal, Paragraph 48.*

things speedier ... I can't imagine it would be costly,'[54] were typical remarks made by participants.

Culture and customs

Another issue raised by a few participants that could inhibit the use of electronic signatures is the culture and custom associated with manuscript signatures. Participants believed that the use of manuscript signatures has become a part of the Australian business culture and custom, and this acts as a significant deterrent to the use of electronic signatures. Relative to an electronic signature, a manuscript signature was considered a 'tried and trusted method of signing documents'[55] for hundreds of years for executing contracts and commercial transactions by the business community. 'A handwritten signature is a cultural thing at the moment,'[56] remarked a participant. 'Things have always been done via pen and paper,'[57] claimed another participant.

Discussion and recommendations

The above section has set out an outline of the various factors that participants identified as potential impediments to the adoption of electronic signature technology. These factors comprise ignorance or lack of understanding of the electronic signature technology and the law governing the technology; security; legal obstacles; complexity and confusion; cost, and culture and customs. Some of these concerns raised are legitimate. For instance, the complex setting-up process of the digital signature technology, the stringent requirement for the recipient organisation to be equipped with a compatible technology or the cost of staff training can result in significant hurdles for businesses. However, several of the concerns raised by participants appear to be unfounded and based on misconceptions.

Ignorance and lack of understanding of the technology was identified as a key impediment to the use of electronic signatures for contracts and commercial transactions in the Australian business community. Because of the lack of awareness, businesses are unable to appreciate the benefits of this technology. It is suggested that they need to recognise that electronic signatures have the capability to enhance their performance and capabilities, and provide them the ease of signing contracts, joint ventures and conduct electronic commerce sitting in front of their computer anywhere in the world.

It is therefore important that resources be provided for training and education programmes for members of staff who are directly or indirectly involved in the use of the electronic signature technology. If the prevailing ignorance, lack of understanding and confusion about the new technology can be addressed, businesses will realise that electronic signatures, in particular digital signatures, can be a secure alternative to manuscript signatures for conducting on-line contracts and commercial transactions. In this respect, the Australian Government Information Management Office (AGIMO) that overlooks the Gatekeeper (which provides accreditation to certification authorities (CAs) to issue digital signature certificates) can play an important role. Other bodies such as the Law Council of Australia (LCA), the Australian Corporate Lawyers Association (ACLA) and the Australian Computer Society (ACS) can also collaborate to promote the use of the technology given its techno-legal nature.

Security concerns were identified as another significant barrier to the use of electronic signatures. In particular, businesses raised concerns with regard to their storage. If electronic signatures are stored properly, their misuse can be minimised. However, participants' views indicated that despite password security policies implemented by their organisation's IT team, staff would not abide by them. Such lackadaisical attitudes towards the use of passwords are in conformity with various studies and surveys that have investigated password security.[58] Such weak passwords can be effortlessly obtained either through the help of social engineering[59] or obtained with the use of software.[60]

On the other hand, replacing passwords with biometric measurements can be a secure option, but is not necessarily a perfect alternative. A computer with an electronic signature stored on its hard disk would most likely be connected at some stage or the other to the internet or an intranet, or both. With the use of either intranet or the internet, there are high risks of remote attacks within an organisation or from a hacker sitting thousands of miles away. Remote attacks can bypass

[54] *P15_C010_Legal, Paragraph 141.*
[55] *P18_C011_Legal, Paragraph 120.*
[56] *P2_C02_Legal, Paragraph 27.*
[57] *P18_C011_Legal, Paragraph 133.*
[58] *Ernst & Young, Global Information Security Survey 2006 at http://www.ey.com/; Steven Furnell, 'Authenticating Ourselves: Will We Ever Escape the Password?' (2005) 3 Network Security 8, 9; Stephen Mason, Electronic signatures in Law, 10.36.*
[59] *For more details on social engineering and password security see Michael E. Whitman, Herbert J. Mattord, Management of Information Security (Course Technology, 2004).*
[60] *Joseph A. Cazier and B. Dawn Medlin 'Password Security: An Empirical Investigation into E-Commerce Passwords and their Crack Times' (2006) 15(6) Information Systems Security 45, 47.*

operating systems security, thereby making any desktop security measures such as biometric measurements, including passwords, redundant.[61] In order to protect electronic signatures from risks associated with the internet or intranet, a possible option is to store them on secure PISDs.[62]

Among all forms of PISD, smart cards appear to be the most secure.[63] However, most participants demonstrated very little understanding of smart cards, particularly the technology associated with them. They were often wrongly believed to be embedded with the magnetic stripe technology, as are most bank credit cards in Australia. Educating the business sector about the technology underlying smart cards might overcome the prevailing ignorance and misunderstanding.[64] To address this issue, the use of biometric measurements may be considered as an alternative to passwords for securing smart cards. While the body is capable of providing several types of biometric measurement, the use of fingerprint has proved itself to be the most suitable technology to date from a security and usability aspect.[65] Thus, it is possible to achieve a higher degree of security by storing a biometric measurement of a fingerprint on the same card that stores a digital signature. A link can be made between the person whose private key is stored on the card and the identity of the person in possession of the card. If such a comprehensive security infrastructure is adopted, digital signatures are protected from malicious acts to the degree that the technology can be considered to be reasonably secure.[66]

Concerns regarding the admissibility of electronic signatures and the evidentiary issues appeared to be another important impediment to the use of electronic signatures in the Australian business community. On the one hand, participants revealed significant ignorance with respect to the law governing electronic signatures in Australia, in particular, the ETA and the law of evidence. The knowledge of lawyers and legal advisors' in this area did not appear to be up-to-date. On the other hand, participants raised some valid arguments with regard to evidentiary matters.

Admissibility concerns raised by participants were in general futile. Both the ETA and the Evidence Act 1995 (Cth) provide rules and guidelines that can be used to prove an electronic signature.[67] Participants' concerns regarding this issue are therefore not exactly tenable. They are mostly characterised by an ignorance of the law underlying electronic signatures. It is arguable that separate provisions on admissibility of electronic signatures in evidence in the ETA would provide more clarity on evidentiary matters related to electronic signatures. On this note, it is useful to point out that the Electronic Communications Act 2000 from the UK, explicitly states that electronic signatures are admissible in evidence in any legal proceedings.[68] The UK Act thus provides a useful model for Australia.

With regard to evidentiary issues, participants expressed concerns about the inconclusiveness of an electronic signature, claiming that there is no actual or original document that is signed. In their contention, the law of evidence would struggle to deal with electronic signatures, because there is an absence of primary evidence.[69] Such views appear to be based on a

[61] *For example, software such as Inspector Copier can remotely back up data from the individual's computer by bypassing the operating system protections.*

[62] *It is possible that electronic signatures stored on a smart card may be susceptible to risks from the internet. This could happen during the process of signing a document, because the smart card is connected to the computer that is in turn connected to the intranet or internet. During this period, a remote attack is possible on the electronic signature. However, since the smart card is in contact with the intranet or internet for only a very short period, this threat is minimal as compared to when electronic signatures are stored on a computer's hard disk which is often connected permanently to the internet or intranet. However, the Network Smart Card can overcome this problem to a considerable extent. See Hong Qian Karen Lu, 'Network smart card review and analysis' International Journal of Computer and Telecommunications Networking Volume 51, Issue 9 (June 2007), 2234-2248 and Joaquin Torres, Antonio Izquierdo and Jose Maria Sierra, 'Advances in network smart cards authentication' International Journal of Computer and Telecommunications Networking Volume 51, Issue 9 (June 2007), 2249-2261.*

[63] *In the past few years smart cards have become more powerful and secure, for which see Bart Preneel, 'A Survey of Recent Developments in Cryptographic Algorithms for Smart Cards' International Journal of Computer and Telecommunications Networking Volume 51, Issue 9 (June 2007) 2223-2233 and Joaquin Torres, Antonio Izquierdo and Jose Maria Sierra, 'Advances in network smart cards authentication' International Journal of Computer and Telecommunications Networking.*

[64] *Note the former federal government was planning to introduce the national identity card that would have used the smart card technology. The intention was to replace a number of existing cards, including the Medicare card and various benefit cards issued by Centrelink and the Department of Veterans' Affairs with the ID card. Had this project been implemented, it would have probably helped users to become familiar with the smart card technology given the broad-based use of Medicare and Centrelink cards. For issues related to such cards see Graham Greenleaf, 'Function Creep – Defined and Still Dangerous in Australia's Revised ID Card Bill' Computer Law & Security Report, Volume 24, Issue 1, 2008, 56-65; Graham Greenleaf, 'Australia's Proposed ID Card: Still Quacking like a Duck' Computer Law & Security Report Volume 23, Issue 2, 2007, 156-166; Margaret Jackson and Julian Ligertwood, 'Identity Management: Is an Identity Card the Solution for Australia?' Prometheus Vol. 24, No. 4. (2006), 379-387.*

[65] *Paul Reid, Biometrics for Network Security (Prentice Hall, 2004) 10.*

[66] *With advances in the smart card technology, it is now possible to have a fingerprint sensor on the smart card itself instead of the computer: 'A standards-based biometric smart card – at what cost?' Biometric Technology Today, Volume 16, Issue 1, January 2008, 3-4; Denis Praca and Claude Barral, 'From smart cards to smart objects: the road to new smart technologies' Computer Networks Volume 36, Number 4, 16 July 2001, 381-389.*

[67] *Sections 8, 9, 10, 11, 12 of the ETA and s 3, 48, 146 of the Evidence Act 1995 (Cth).*

[68] *Electronic Communications Act 2000 (UK) s 7(1).*

[69] *For a discussion on primary and secondary evidence in the context of electronic signatures, see Stephen Mason, Electronic Signatures in Law, 14.10.*

In any event, notaries across the world have taken practical steps to develop techniques to provide for the witnessing the signing of a digital document on a computer with an electronic signature by both the signing party and the notary.

misunderstanding of the current law of evidence. Although the common law position enunciated over 250 years ago was that the best evidence rule[70] (which includes producing original documents containing signatures) should be followed to determine the existence of a signature, this law no longer prevails in the Australian federal and in several state jurisdictions.[71] Because s 51 of the Evidence Act 1995 (Cth) has abolished the common law principles of the best evidence rule for proving a document's contents, the production of an original document is no longer a mandatory requirement to prove a fact. Thus, participants' concerns with regard to the absence of original documents with electronic signatures are unfounded and emanate from their lack of awareness of the current legal position in this regard.

With regard to witnessing the application of a signature, participants feared that unlike manuscript signatures, it is not possible to witness a person affix an electronic signature to a document.[72] Witnessing in the electronic realm has also been described as a complex issue by a few scholars.[73] However, they do not rule out the possibility of witnessing an electronic signature, in particular, digital signatures. Witnesses can use their digital signature to attest an electronically signed document. The witnessing of such documents would require that computers involved in signing the document be technically evaluated to trusted evaluation criteria.[74] In such an environment, the attester would verify the authenticity of the document through the signer's public key and would in turn witness the signatory's signature using his digital signature.[75] In any event, notaries across the world have taken practical steps to develop techniques to provide for the witnessing the signing of a digital document on a computer with an electronic signature by both the signing party and the notary.[76]

The issue of witnessing has been explicitly provided for in a few jurisdictions' legislation. For example, the Electronic Commerce Act 2000 passed in Ireland, provides that electronic signatures can be witnessed electronically provided certain requirements are satisfied. In particular, the main document must specify that it requires witnessing, and the signature of the signatory and the witness must be an advanced electronic signature (that is, a digital signature) based on a qualified certificate.[77] The Electronic Transactions Act 2002 in New Zealand also makes explicit provisions for the witnessing of electronic signatures.[78] A similar provision if inserted in the ETA will eliminate the

[70] *The best evidence rule can be traced back to more than 250 years to the case of Omychund v Barker (1745) 26 ER 15, 33. Lord Harwicke in the case stated that for evidence to be admissible it must be 'the best that the nature of the case will allow'. In other words the contents of a document are only admissible if the party attempting to adduce evidence of the contents is able to tender the original document. Traditionally, this rule has operated to eliminate evidence which has not been the best evidence, such as a copy of a document. This was basically the issue raised by participants when they expressed concerns about the original and copy of a signature. For a detailed understanding of the best evidence rule see Edward W Cleary and John W Strong, 'The Best Evidence Rule: An Evaluation in Context' (1965) 51 Iowa Law Review 825.*

[71] *The States and Territories in which the best evidence rule has been abolished are New South Wales, Victoria, Australian Capital Territory and Tasmania. Note that these States and Territories mirror the Evidence Act 1995 (Cth). See ss 48 and 51 of the Evidence Act 1995 (Cth). The States and Territories in which the best evidence rule are still active are South Australia, Western Australia, Northern Territory and Queensland.*

[72] *Although see the US case of an electronic will, Taylor v Holt CA Tennessee Knoxville 18 August 2003, where the electronic signature of the testator was witnessed by the witnesses, who in turn added their electronic signatures to the document; discussed in Stephen Mason, Electronic Signatures in Law, 10.16.*

[73] *Adrian McCullagh, Peter Little, and William J Caelli, 'Electronic Signatures: Understand the Past to Develop the Future' (1998) 21(2) University of New South Wales Law Journal 452, 462.*

[74] *Adrian McCullagh, Peter Little, and William J Caelli, 'Electronic Signatures: Understand the Past to Develop the Future'. A lack of trusted systems may bring into question the legal validity and certainty of such actions.*

[75] *Adrian McCullagh, Peter Little, and William J Caelli, 'Electronic Signatures: Understand the Past to Develop the Future'.*

[76] *By way of introduction, see the work of the Hague Conference on Private International Law and the e-APP (Electronic Apostille Pilot Program) http://www.e-app.info/.*

[77] *Electronic Commerce Act 2000 (Ireland) s 14.*

[78] *Section 23 of the Electronic Transactions Act 2002 (NZ) specifically entails provisions for witnesses to witness a document using an electronic signature, if: (a) where a signature is being witnessed, that signature is also an electronic signature; and (b) the electronic signature of the witness meets requirements that correspond to those for a primary signature – that is, the electronic signature adequately identifies the witness and adequately indicates that the signature or seal has been witnessed; is as reliable as is appropriate given the purpose for which, and the circumstances in which, the signature of the witness is required; and, in the case of a witness's signature on information required to be given to a person, the recipient of the information has consented to the use of an electronic signature rather than a traditional paper-based signature.*

concerns of the Australian business community that electronic signatures and documents cannot be witnessed.

Electronic signatures were also subject to disapproval because they cannot undergo handwriting tests. Participants claimed that unlike manuscript signatures which can be verified using handwriting tests,[79] identifying the actual signatory becomes harder when an electronic signature is used. However, there are other ways of testing whether an electronic signature is genuine and authorized. The operations of the information system from which the signature originated at the time when the signature was created can be used to prove the genuineness of a signature.[80] Further, intrusion detection systems may be used to establish whether the document was signed maliciously by an intruder.[81] This may however require a high standard of information security systems. Nevertheless, this may not necessarily be a foolproof means to identify the actual signatory. In the case of electronic signatures, the identity of the actual signatory will be a matter of inference. Inference may be weak in those cases where the holder of the private keeps his key in a computing platform that cannot be trusted, such as an office or home computer.[82] The inference may be stronger in those cases where better evidence of a signer's identity has been provided through a biometric measurement and a PISD or both.[83]

Some participants claimed that businesses would willingly switch over from the practice of manuscript signature to electronic signatures for endorsing contracts and documents if they received adequate legal advice. Providing adequate legal advice is, however, quite challenging for legal advisors if there are fundamental drawbacks in the electronic signature legislation. A major shortcoming of the ETA is that it does not provide the definition of an electronic signature.[84] This can be rectified if the Act is amended to incorporate the definition of electronic signature and digital signature. Other countries such as Hong Kong have already implemented such changes in their legislation.[85] Similar amendments in the ETA will help the Australian business community and other people that use electronic signatures every day (the PIN on a bank or credit card, the signature at the bottom of an e-mail) understand what an electronic signature represents. Clarity in the legislation is in turn likely to enhance businesses' confidence towards the use of the technology.

Furthermore, section 10 of the ETA (based on article 7 of the MLEC) that deals with the use of signatures in the electronic environment, recognises the validity of electronic signatures under certain terms and conditions without describing what an electronic signature is. In particular, it states that where a Commonwealth law imposes the completion of a transaction through the means of a signature, the use of any method (presumably electronic signature) is valid, provided the method satisfies the following four criteria:

> it identifies the person who made the signature;
> it indicates the person's approval to the contents of the document signed;
> it is as reliable as is appropriate for the purpose for which it is used; and
> the recipient has agreed to the usage of that method.[86]

Clearly, this section is vague and ambiguous, making it difficult to attribute a precise meaning to its provisions, and is the subject of criticism from scholars eminent in the field of electronic signatures. McCullagh and Caelli condemned the legislation on the ground that it does not provide 'any guidance as to what within the electronic commerce environment is or is not a valid electronic signature'.[87] According to Christensen and Low, that 'the method must be as reliable as is appropriate for the purpose for which the information was communicated'[88] is nothing but confusing.[89] What is considered appropriate in the circumstances, argued

[79] *Generally two main aspects of a signature are considered: pictorial representation and the construction of letters. It is common for forgers to focus on pictorial details such as slope, size and spacing but they often fail to copy the way the letters are constructed, such as the direction of the letters. In addition, the signature is also verified on the basis of the attributes of the instrument used to affix the signature such as how smooth the signature has been signed and whether it is jagged or confident. See Stephen Mason, Electronic Signatures in Law, 1.17.*

[80] *Lorna Brazell, Electronic Signatures Law and Regulation (Sweet & Maxwell, 2004), 8-014.*

[81] *Lorna Brazell, Electronic Signatures Law and Regulation, 8-014. Note intrusion detection systems can only detect intrusions but cannot prevent them.*

[82] *Mark Sneddon, Legal Liability and E-Transactions: A Scoping Study for the National Electronic Authentication Council (2000) 3.2, available at http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN014676.pdf.*

[83] *Mark Sneddon, Legal Liability and E-Transactions: A Scoping Study for the National Electronic Authentication Council (2000).*

[84] *Fitzgerald and others argue that ETA is a light-touch legislation because it does not define the electronic signature: Anne Fitzgerald, Timothy Beale, Yee Fen Lim and Gaye Middleton, Internet and E-Commerce Law, (Lawbook Co., 2007) 552.*

[85] *Electronic Transactions (Amendment) Ordinance 2004 (HK).*

[86] *ETA s 10. Note the clause 'the recipient has agreed to the usage of that method' is an extra provision in the ETA as compared to the MLEC.*

[87] *Adrian McCullagh and William J Caelli, 'Non-repudiation in the Digital Environment' (2000) 5(8) First Monday http://firstmonday.org/issues/issue5_8/mccullagh/index.html.*

[88] *ETA s 10.*

[89] *Sharon A Christensen, William Duncan and Rouhshi Low, 'The Statute of Frauds in the Digital Age - Maintaining the Integrity of Signatures' (2003) 10(4) Murdoch University Electronic Journal of Law http://www.murdoch.edu.au/elaw/issues/v10n4/christensen104.html.*

Christensen and Low, could be based on the parties' personal preferences and a court's ex-post facto rationalisation of individual approaches, and therefore could vary greatly with no consistent pattern.[90] For example, the appropriateness of an electronic signature may not be the same for a day-to-day ordinary transaction as for complex business transactions involving large sums of money.

In the same vein, Mason argued that the reliability test is unrealistic. According to him, if the parties to a contract have agreed in good faith on a particular technology and have acknowledged that the contract is authentic and valid, the court should not question its authenticity and validity on the grounds of reliability. 'There should be no need for any court to take the matter any further,' remarked Mason.[91]

The lack of clarity in the provisions relating to signatures in the electronic environment is a major drawback in the ETA and other jurisdictions whose electronic transactions laws are based on the MLEC. It would indeed be hard for legal advisors to advise businesses to use electronic signatures with such loose, imprecise and ambiguous provisions in the laws. Note that post MLEC, two other set of laws, the Model Law on Electronic Signatures 2001 (MLES) and the Convention, have been drafted by the UNCITRAL that address the drawbacks in the initial model law but to date the ETA has not been amended accordingly.

The complexity of the electronic signature, in particular digital signature, was regarded as another hindrance to the use of electronic signatures by participants. However, the complexity of the technology can also optimistically be regarded as an attribute. Seen from a different perspective, due to its complex nature, digital signatures can only be used by authorized people who have acquired an expertise or training in this respect. Thus, the complexity of the technology can potentially enhance its security by restricting its use.[92]

It appears that much of businesses' confusion with electronic signatures arises from an ignorance or lack of understanding of the technology. The electronic signature technology, in particular digital signatures, is not necessarily as complex as it is perceived. This perceived complexity is often the result of poor understanding and lack of information.

Economically, the expense involved in educating and training staff was identified as an important deterrent towards the use of digital signatures by participants. However, businesses may reconsider that the use of digital signatures may justify the expenses involved in their use, because of the slightly greater security. Although in the short run they may incur certain expense in terms of training and educating their staff, the long run it is possible that the gains might outweigh the expenses.

Conclusion

This article identifies the potential reasons underlying Australian businesses' hesitance to use electronic signatures, in particular digital signatures, for contracts and commercial transactions in a fast developing and regulated e-environment. It also provides some useful suggestions to overcome the low use of the technology in the business community. While legislative and technological shortcomings are identified as being important factors that can make businesses hesitant to adopt electronic signatures, the perception of people in business are often not supported by reference to the actual legislation or to the technology underlying electronic signatures. Rather, there is significant evidence of Australian businesses' lack of awareness and understanding of electronic signatures and the associated legislation, despite a regulatory framework to facilitate their use. It is unlikely that any perfection of either electronic signature technology or the legal environment for electronic signatures will see a greater use by the business community of such signatures until knowledge of these things becomes more pervasive.

Dr. Aashish Srivastava is in the Department of Business Law and Taxation, Monash University, Australia. His doctoral thesis comprised an empirical research on the lack of acceptance of electronic signatures by the Australian business community. His research interests include legal issues in electronic signatures, e-government, internet security and cyber crimes.

aashish.srivastava@buseco.monash.edu.au

[90] *Sharon A Christensen, William Duncan and Rouhshi Low, ' The Statute of Frauds in the Digital Age - Maintaining the Integrity of Signatures'.*

[91] *Mason's argument is in the context of article 7 of the Model Law on Electronic Commerce 1996, which can also be applied to ETA because s 10 of the ETA is a replication of article 7 of the model law. Stephen Mason, Electronic Signatures in Law, 3.18.*

[92] *Some commentators consider digital signatures to be the most secure form of electronic signature, although a number of companies in Russia bear witness to having large sums of money removed from their bank accounts by an unknown unauthorized third party, who obtained the private key of the company, and then initiated the transfer of the money without the authority or knowledge of the company, for which see Olga I. Kudryavtseva, ' The use of electronic digital signatures in banking relationships in the Russian Federation' , Digital Evidence and Electronic Signature Law Review, 5 (2008) 51 – 57 and Resolution of the Federal Arbitration Court of Moscow Region of 5 November 2003 N КГ-А 40/8531-03-П, Digital Evidence and Electronic Signature Law Review, 5 (2008) 149 – 151.*

