

# Legal Issues in Storing and Producing Electronic Records

## Victorian Records Management Network October 2002

Mark Sneddon, Partner  
[msneddon@claytonutz.com](mailto:msneddon@claytonutz.com)

Sven Bluemmel, Senior Associate  
[sbluemmel@claytonutz.com](mailto:sbluemmel@claytonutz.com)

Clayton Utz

CLAYTON UTZ

# *Document Retention Requirements*

- ◆ Legislation:
  - *Public Records Act 1973*
  - *Information Privacy Act 2000*
  - *Health Records Act 2001*
- ◆ Evidentiary issues in the case of disputes or challenges to a process. Issues:
  - Admissibility of evidence
  - Weight of evidence
- ◆ Good administrative practice

# *Electronic Transactions Acts*

- ◆ Commonwealth *Electronic Transactions Act 1999*
- ◆ *Electronic Transactions (Victoria) Act 2000* commenced 1 September 2000 - covers all Vic laws (including common law) unless exempted by regulation
- ◆ Parallel legislation in all other States and Territories (except WA) – in operation everywhere but SA (1/11/02) and QLD

# *Electronic Transactions Acts*

- ◆ Transactions not invalid under relevant law simply because they use electronic communications or electronic signatures
- ◆ Electronic communication can be used where a relevant law requires or permits a person to give information in writing

# *Electronic Transactions Acts*

- ◆ Electronic authentication can be used in place of a handwritten signature if a communication needs to be signed under relevant law
- ◆ Default rules for determining the time and place of dispatch and receipt of electronic communications

# *Electronic Transactions Acts*

- ◆ Records required or permitted to be produced or retained under law can be produced or retained electronically if:
  - the method of generating the electronic form provided a reliable means of assuring the maintenance of the integrity of the information contained in the document, and
  - the information has remained complete and unaltered except for the addition of endorsements and immaterial changes in the ordinary course of communication, storage or display

# *Electronic Transactions Acts*

- ◆ For retention requirements, regulations may require that the information be recorded on a particular kind of data storage device
- ◆ For required retention of information in electronic communications for a required period, throughout the period the record keeper must retain, in electronic form, additional info to identify:
  - Origin and destination of the electronic communication
  - Time the communication was sent and received

# Archiving and Time Stamping of Records

- ◆ Relevant issues include:
  - degradation of storage medium/periodic migration to new media
  - degradation of key security (cf advances in cryptanalysis)/re-signing of records
  - scope and reliability of time stamping
  - retention and backward compatibility of relevant hardware and software

# Electronic Records as Evidence

- ◆ Rules for admissibility of electronic records as evidence are not uniform throughout Australia – there is a risk of inconsistent decisions
- ◆ Current *Evidence Act 1958 (Vic)* predates the widespread use of electronic documents:
  - Best evidence rule
  - Rule against hearsay
- ◆ Business records exemption

# Electronic Records as Evidence

- ◆ An agency's electronic records may be admissible as "computer generated records" or "business records" *of what the agency received or stored* but not necessarily of the electronic document that was sent or how it was created
- ◆ Need for cooperation with software developers to ensure that electronic documents received are reliable records of what was created, signed and sent
- ◆ Electronic witnessing is a particularly difficult area

# ETA - Issues To Watch

- ◆ Care in selection and retention of technology for storing, retrieving and reading electronic records
- ◆ Consent to receiving electronic communications and signatures - refuse consent to all but specified platforms
- ◆ Witnessing, negotiable instruments
- ◆ Watch for possible exemptions in regulations - eg wills, affidavits, personal service, other jurisdictions eg Corps Act

# Uses of Signatures for Security

- ◆ Authenticating messages / consents (eg online lodgment, tenders)
- ◆ Access Control for security and privacy (eg to database, patient records)
- ◆ Authenticating servers, webpages, documents, programs
- ◆ Audit trails and accountability, archiving and tamper-proofing e-records
- ◆ Providing proof for legal proceedings (eg document integrity, identity of signer)

# Legality of E -Signatures

- ◆ Legal questions over e-signatures mainly where statutes require (manual) signature
- ◆ Electronic Transactions Acts largely fix this but non-uniform exceptions
- ◆ ETA e-signatures
  - Identify person and indicate approval
  - reliable as appropriate for purposes of the communication
  - consent of recipient (can be implied) – if Cth - meet specified IT requirements

# Legal Liability and Reliability of E-Signatures

- ◆ The security and features of end user implementation are as critical as the core identification technology (eg PKI), ie. storage of keys, passwords, signing mechanisms, certificate management and validation software
- ◆ Analyse the strength of an authentication system by the weakest link (security of the private key)
- ◆ Signature method/device for PKI
  - on a hard drive
  - smart card and PIN - plus CA change!

# Digital Signature Liability Issues (cont'd)

- ◆ Contract re risk with “providers” eg outsourced IT manager, security solutions provider, CA.
- ◆ Liability of CAs to Subscribers and Relying Parties
  - see Clayton Utz Report to NEAC:  
[www.claytonutz.com/fr-ecomm.htm](http://www.claytonutz.com/fr-ecomm.htm) and on NOIE site

# PKI - Relying Party Security Weakness

- ◆ Non-robust certificate validation software and processes eg MS Outlook
- ◆ ‘Planting’ of certificates in browsers
- ◆ Inadequate notice to RPs by software
- ◆ Out of date CRLs, is OCSP available?
- ◆ Signature stripping - TTP archiving solution

# Privacy

- ◆ Information Privacy Act 2000 and Health Records Act 2001
  - data security requirements for agencies in addition to other secrecy and confidentiality provisions
  - Destroy or de-identify when no longer needed subject to *Public Records Act*
  - *Health Records Act* – health service providers must retain health information for 7 years or longer

# Privacy and Data Security

- ◆ Privacy Compliance a significant project
  - More than putting up a privacy policy
  - Need to review information flows into, out of and within the organisations and audit current practices against IPPs and HPPs
  - Dovetail with audit of IT/data security/access/quality, IT user policies and archiving procedures
  - Clayton Utz compliance tools used with a range of public and private sector organisations

# Conclusion

- ◆ Do a careful security risk assessment of e-record management and e-signature offerings – how reliable?
- ◆ Do a legal assessment - who bears risks of security compromise/error? Allocate by contract eg. IT provider, counterparty, CA
- ◆ Do a costs-benefit analysis - does the ‘solution’ solve enough for its price?  
Factor in archiving/back up/disaster recover and counterparty costs and retained risks

# Legal Issues in Storing and Producing Electronic Records

## Victorian Records Management Network October 2002

Mark Sneddon, Partner  
[msneddon@claytonutz.com](mailto:msneddon@claytonutz.com)

Sven Bluemmel, Senior Associate  
[sbluemmel@claytonutz.com](mailto:sbluemmel@claytonutz.com)

Clayton Utz

CLAYTON UTZ