Technology Law

Information Technology Litigation

peguambela dan peguamcara

Vello Kader & Shah

advocates and solicitors

Introduction

- Understanding the Internet
- Understanding the World Wide Web
- Understanding a Computer

WHY IS THIS IMPORTANT?

"access"

peguambela dan peguamcara
Vello Kader & Shah
advocates and solicitors

The Internet

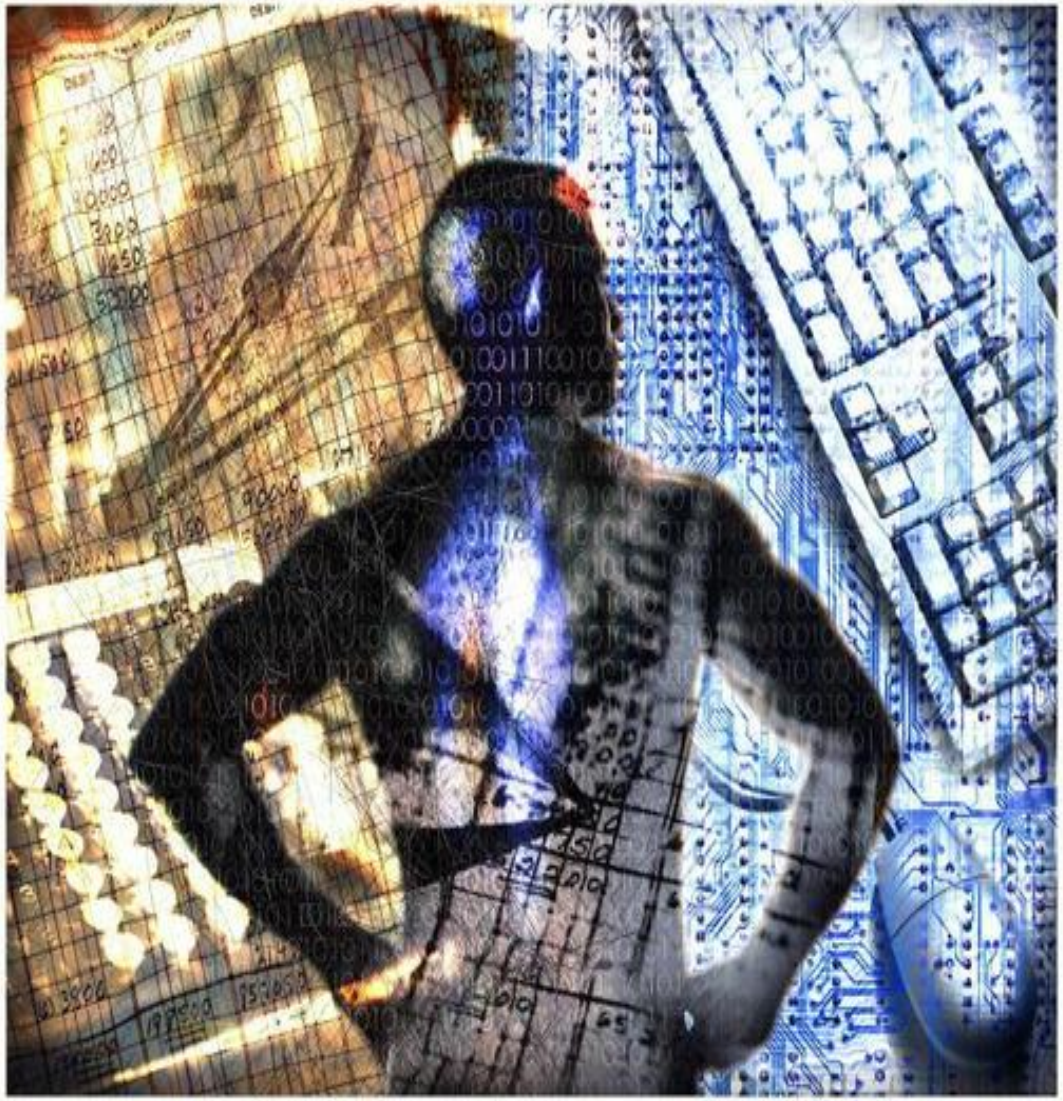
- Network or networks developed in the 60's. Originally known as the ARPANET. Used mainly for the military and education.
- Comprises the infrastructure, its functions and the parties who use it and apply it.
- Web of software protocols known as the TCP/IP, a communication protocol.
- An architecture which allows traffic such as email, instant messaging, VOIP, www, etc..

The World Wide Web

- Internet application developed in 1980 by Tim Berners Lee using the “http”.
- Web online services such as email, payment systems, shopping, banking, insurance, gaming, gambling, advertising, social media applications, online media, online library, etc etc.

The Computer

- "an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, storage and display functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include an automated typewriter or typesetter, or a portable hand held calculator or other similar device which is non-programmable or which does not contain any data storage facility"



Electronic Evidence / Digital Evidence

Computer Information

peguambela dan peguamcara
Vello Kader & Shah
advocates and solicitors

Electronic Evidence

- Nature of electronic evidence is such that it exists in many different places at the same time and thus difficult to completely remove such evidence.
- At the same time, due to the characteristics of information technology, may be difficult for investigators to discover and collect evidence.
- Most important characteristic of an electronic version of a document is that it may not be identical to the printed copy.
- Significant hidden information may only be visible during an examination of the electronic version.
- The electronic copy of a document would therefore contain more information than a supposedly complete printout of the same document.
- Electronic data is more vulnerable than paper-based documents.

Communication of Information

- Emails - Web based
- Short Messaging Service on the Internet;
- Social media applications for eg Twitter, Facebook, Friendster;
- Chat applications - yahoo, msn, skype, etc.

Computer Generated Documents

- Documents created / printed from a computer for eg. an email.. “electronic version”
- Copies vs Original?
- Possibility of tampering?
- Authentication?
- Digital Signature? DSA 1997
- Admissible?

Admissibility

- When objection taken, admissibility is at issue?
- S.90A Evidence Act 1955;
- Weight of evidence to be attached;
- Computer forensics?

Computer Forensics

- Why?
- Necessary?
- Courts view?
- Expert witness? Accreditation - CISSP
- Cyber Security - Govt Forensic Dept

- Source and reliability of the information needs to be assessed.
- Extraction, examination, preservation and presentation.
- Chain of custody must be preserved to ensure that there was no tampering.
- Examples of points to be reported in the report by the forensic examiner:-
  - a. who collected the evidence;
  - b. how and where the evidence was collected;
  - c. name and person who took evidence;
  - d. how and where the evidence was stored;

peguambela dan peguamcara
Vello Kader & Shah
advocates and solicitors

- e. notes prepared during the examination phase of the investigation;
- f. details about the way the investigation was conducted;
- g. validity of procedures involved;
- h. details of discovery;
- i. other relevant evidence;
- j. possibility of concoction.

Legislation

- Digital Signatures Act 1997
- Computer Crimes Act 1997
- Communications & Multimedia Act 1998
- Evidence Act 1950

Digital Signatures Act

- CAIN Principles - Confidentiality, Authentication, Integrity & Non-Repudiation.
- Technological tool using encryption as a means to ensure security.

Computer Crimes Act

- An Act (only legislation) that addresses computer crimes and provides liabilities and punishments attached to it.

- Presents a number of obstacles to forensic investigators.
  - These obstacles are actually aimed at deterring hackers from accessing, copying and or damaging computers or computer data;
  - Offences may be committed by an investigator during his course of investigations.
  - Whether or not this happens, would depend upon who accesses the computer and data, who owns the computer, where the computer is located, under what conditions and how access to the computer is gained, the existence of either a warrant or other court order granting such access and express or implied ownership of copyright.

The Section Offences

- Section 3: Unauthorised access to computer material;
  - » Fine not exceeding RM50,000.00 or to imprisonment for a term not exceeding 5 years or both.
- Section 4: Unauthorised access with intent to commit or facilitate commission of further offences;
  - » Fine not exceeding RM150,000.00 or to imprisonment for a term not exceeding 10 years or to both.
- Section 5: Unauthorised modification of computer material.
  - » Fine not exceeding RM100,000.00 or to imprisonment for a term not exceeding 7 years or to both and if the act is done with the intention of causing injury as defined in the Penal Code, then a fine not exceeding RM150,000.00 or to imprisonment for a term not exceeding 10 years or to both.
- Section 6: Wrongful Communication
  - » Fine not exceeding RM25,000.00 or to imprisonment for a term not exceeding 3 years or both.
- Section 7: Abetments and attempts
  - Any term of imprisonment imposed shall not exceed one-half of the maximum term provided for the offence.

S.233 Communications & Multimedia Act

- (1) A person who -
  - (a) by means of any network facilities or network service or applications service knowingly -
    - (i) makes, creates or solicits; and
    - (ii) initiates the transmission of,

    any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person; or

    (b) Initiates a communication using any application service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threaten or harass any person at any number or electronic address,

    COMMITS AN OFFENCE

peguambela dan peguamcara
Vello Kader & Shah
advocates and solicitors

S.114A Evidence Act "Presumption of fact in publication"

- (1) A person whose name, photograph or pseudonym appears on any publication depicting himself as the owner, host, administrator, editor or sub-editor, or who in any manner facilitates to publish or re-publish the publication is presumed to have published or re-published the contents of the publication unless the contrary is proved.

- (2) A person who is registered with a network service provider as a subscriber of a network service on which any publication originates from is presumed to be the person who published or re-published the publication unless the contrary is proved.

- *Q: How does one find out details of registration of a subscriber of a particular network service?*

- (3) Any person who has in his custody or control any computer on which any publication originates from is presumed to have published the content of the publication unless the contrary is proved.

Courts Approach

- How do Judges view these cases?
- What is required of counsel to advise the Court?
- Evidentiary aspect?
- Need for a computer forensic expert?
- Presentation to Court.

Recent Amendments

- Evidence Act Amendments
- Dispensing the need of proving but requires a higher standard of disproving.
- How will the Courts view / accept this?
- Failed to address pertinent point - "***human intervention***" = authentication, reliability and integrity. Eg, S.404 Sarbanes Oxley
- Is there an overwhelming inference as to the authenticity of a document?

Authentication

- Capacity to prove the digital object is what is purports to be, the authenticity of a digital object is preserved by the use of techniques to prevent the data from being manipulated, altered or falsified deliberately or inadvertently. Such methods include providing audit trails of transmissions and maintaining records or encryption. A number of attributes, taken together, provide evidence of authenticity - the way in which data is preserved and the manner in which it is managed. - See Electronic Evidence: Disclosure, Discovery and Admissibility - Page 94 Para 4.28 (a)

Integrity

- Relates to how sound the data is, such as whether the data is damaged in some way, and whether it is complete, in that is possesses all the necessary parts and links. Integrity is not an absolute condition but a state of relationships, and whether the burden of proof will be achieved in any individual case will depend on the strength of the relationships to the data. - See Electronic Evidence: Disclosure, Discovery and Admissibility - Page 94 Para 4.28 (b)

Reliability

- The capacity of a digital object to stand for the facts to which it purports to attest, which, in turn, is linked to ensuring sufficient procedural and technical attributes are in place and working to provide for a degree of assurance that the digital object can be deemed to be reliable. In essence, reliability is associated with the degree of control exercised over the procedures that permit the date to be created. - See Electronic Evidence: Disclosure, Discovery and Admissibility - Page 94 Para 4.28 (c)

Appreciation

- Lawyers who chose to ignore these new developments in law may subject themselves to malpractice claims. - Alan Gahtan on Electronic Evidence
- Lawyers and prosecutors should ensure that proper authorities are produced in Court to ensure that development of the law can continue. They represent the forefront in any area of development of the law.
- Continuing Legal Education is paramount. Should also include the judiciary.

- The End….

  - » Thank you… Have a great weekend..
  - » E: ravinvello@gmail.com

peguambela dan peguamcara
Vello Kader & Shah
advocates and solicitors