

International Seminar
DIGITAL RECORDS
AND LEGAL ADMISSIBILITY
2024



Mr. Chow Siang Kong
The Attorney General's Chambers (AGC)

Digital Evidence Admissibility for Legal Proceedings in Malaysia



DIGITAL EVIDENCE ADMISSIBILITY FOR LEGAL PROCEEDINGS IN MALAYSIA

CONTENTS

01

INTRODUCTION

02

THE SOURCE OF DIGITAL EVIDENCE

03

MALAYSIA EVIDENCE ACT

04

DIGITAL EVIDENCE & MALAYSIA EVIDENCE ACT

05

SECTION 90A, 90B & 90C EVIDENCE ACT 1950

06

CHALLENGES ON THE ADMISSIBILITY

07

PRESERVATION OF DIGITAL EVIDENCE

08

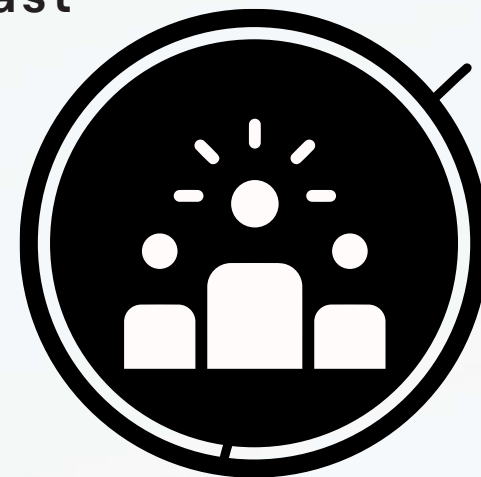
WAY FORWARD



INTRODUCTION

IR4W

Datuk Seri Anwar Ibrahim, Prime Minister of Malaysia, said: "Malaysia is honored to be part of the global network of Centres for the Fourth Industrial Revolution with the first Centre for 4IR in Southeast Asia."



Court Digitalization

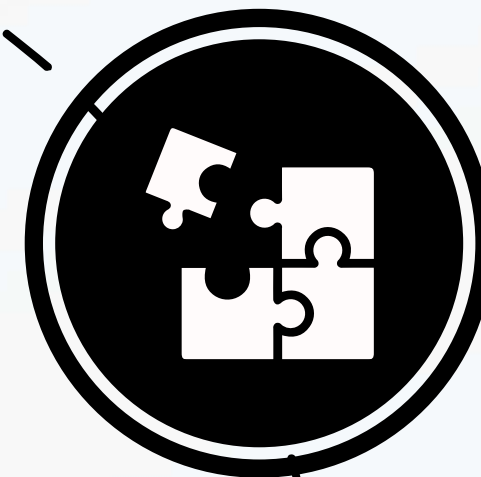
Video Conference/ live video/ live television link

E-Jamin
E-Filing System
E-PG
E-Review
Cyber Court



Legislation

Electronic Commerce Act 2006
Electronic Government Activities Act 2007
Evidence Act 1950
Cybersecuritu Act 2024



Sources of Digital Evidence

- Computer
- Hardware
- Software
- System software
- Clock



Electronic Storage
Information

Types of data



ACTIVE DATA



ARCHIVAL DATA



RESIDUAL DATA



METADATA

ACTIVE DATA

- Work in progress
- email messages
- word processing document
- spreadsheets
- databases
- calendars



ARCHIVAL DATA

- information that is no longer in continuous use.
- created automatically as a backup in cases where the user fails to save.
- The document can be recovered even after it has been deleted if it is preserved on the user's hard drive.

REPLICANT DATA

- Replicant data can be commonly found in printer memories, unsaved data that is sent to printer
- such data still can still be accessed in the event of a system failure.

RESIDUAL DATA

- Residual data is information that has been deleted but continues to remain in the system.
- A computer forensics expert would still be able to recover file fragments from deleted files that have only been partially overwritten.

EMBEDDED DATA/ METADATA

- Metadata is data that is automatically created and stored by computer programs that is not visible in the hardcopy paper document.
- Metadata is important when examining a word processing documents and emails as the only method of authenticating the sender, route and content.

Search of data- s.116 CPC

(1) Whenever a police officer making a police investigation considers that the production of any document or other thing is necessary to the conduct of an investigation into any offence which he is authorised to investigate and there is reason to believe that the person to whom a summons or order under section 51 has been or might be issued will not or would not produce the document or other thing as directed in the summons or order or when the document or other thing is not known to be in the possession of any person, the officer may search or cause search to be made for the same in any place.

(2) That officer shall, if practicable, conduct the search in person.

(3) If he is unable to conduct the search in person and there is no other person competent to make the search present at the time, he may require any officer subordinate to him to make the search, and he shall deliver to the subordinate officer an order in writing specifying the document or other thing for which search is to be made and the place to be searched, and the subordinate officer may then search for the thing in that place.

(4) The provisions of this Code as to search warrants shall, so far as may be, apply to a search made under this section.



Search & seizure without warrant s.116A CPC

(1) Whenever it appears to any police officer not below the rank of Inspector that there is reasonable cause to suspect that there is concealed or deposited in any place any evidence of the commission of a security offence or any offence relating to an organized crime and such police officer has reasonable grounds for believing that, by reason of delay in obtaining a search warrant, the object of the search is likely to be frustrated, he may-

(a) enter any premises and there search for, seize and take possession of, any book, document, record, account or data, or other article;

(b) inspect, make copies of, or take extracts from, any book, document, record, account or data;

(4) For the purpose of this section, "security offence" means a security offence as specified under the First Schedule to the Security Offences (Special Measures) Act 2012 [Act 747]




Access to computerized data- s.116B CPC


- (1) A police officer not below the rank of Inspector conducting a search under this Code shall be given access to computerized data whether stored in a computer or otherwise.
- (2) Any information obtained under subsection (1) shall be admissible in evidence notwithstanding any other provisions in any written law to the contrary.
- (3) For the purpose of this section, "access" includes being provided with the necessary password, encryption code, decryption code, software or hardware and any other means required to enable comprehension of the computerized data.





Interception of communication and admissibility of intercepted communications s.116C CPC

- (1) Notwithstanding any written law to the contrary, the Public Prosecutor, if he considers that it is likely to contain any information relating to the commission of an offence, may authorize a police officer—
 - (a) to intercept, detain and open any postal article in the course of transmission by post;
 - (b) to intercept any message transmitted or received by any communication; or
 - (c) to intercept, listen to or record any conversation by communication.
 - (2) The Public Prosecutor, if he considers that any communication is likely to contain any information relating to the commission of an offence, may—
 - (a) require a communications service provider to intercept and retain a specified communication or communications of a specified description received or transmitted, or about to be received or transmitted by that communications service provider; or
 - (b) authorize a police officer to enter any premises and to install on such premises, any device for the interception and retention of a specified communication or communications of a specified description and to remove and retain such device.
 - (3) Where any person is charged with an offence, any information obtained under subsection (1) or (2), whether before or after such person is charged, shall be admissible in evidence at his trial.
 - (4) An authorization by the Public Prosecutor under this section may be given either orally or in writing, but if an oral authorization is given, the Public Prosecutor shall as soon as practicable reduce the authorization in writing.
 - (5) The Court shall take cognizance of any authorization by the Public Prosecutor under this section.
- 




Evidence Act 1950

An Act to define the law of evidence.

01. Relevancy of
facts

02. Documentary
Evidence

03. ADMISSIBILITY OF EVIDENCE
OBTAINED UNDER MUTUAL
ASSISTANCE IN CRIMINAL
MATTERS REQUESTS



Relevancy



- Fact must be relevant to the issue
- Relevancy provisions s.6 - s.57 Evidence Act 1950.
- Admissibility evidence subject to probative effects against prejudicial effects.



The Best Evidence Rules



- Best evidence available.
- Probative value depending on offered as real evidence or establishing the truth of contents.
- Admissibility evidence subject to probative effects against prejudicial effects.
- s.62 Explanation 3 Evidence Act 1950.
- Secondary evidence can be admitted in place of primary evidence



The Rule Against Hearsay



- Evidence at trial should be in the form of sworn statement.
- The witness who has personal knowledge of the facts being presented.
- As a general rule, hearsay evidence is inadmissible..
- computer data is not often entered by a person with personal knowledge on the matters
- Hearsay evidence is admissible as long as it is shown to be reliable and its admission is necessary.



Exception- Opinion Evidence



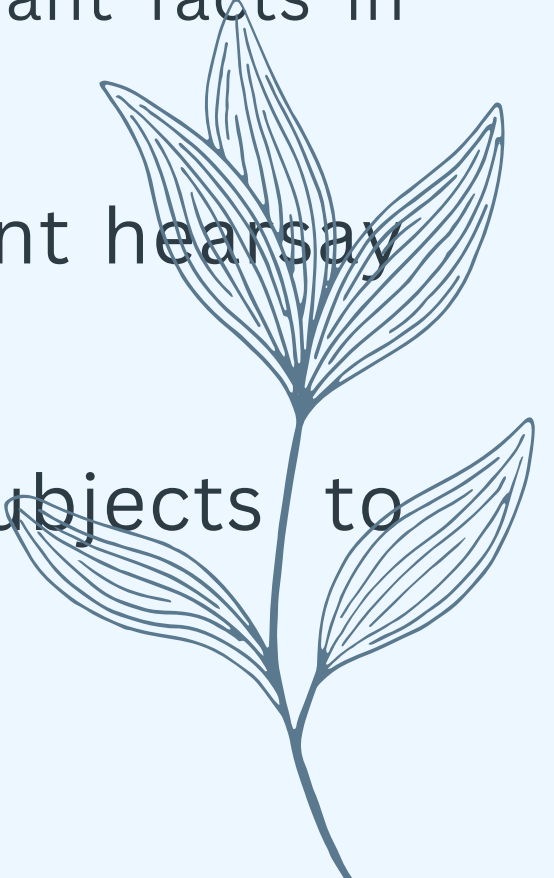
- s. 45 Evidence Act 1950
- (1) When the court has to form an opinion upon a point of foreign law or of science or art, or as to identity or genuineness of handwriting or finger impressions, the opinions upon that point of persons specially skilled in that foreign law, science or art, or in questions as to identity or genuineness of handwriting or finger impressions, are relevant facts.
- (2) Such persons are called experts.



Exception- s,32(1) Evidence Act 1950



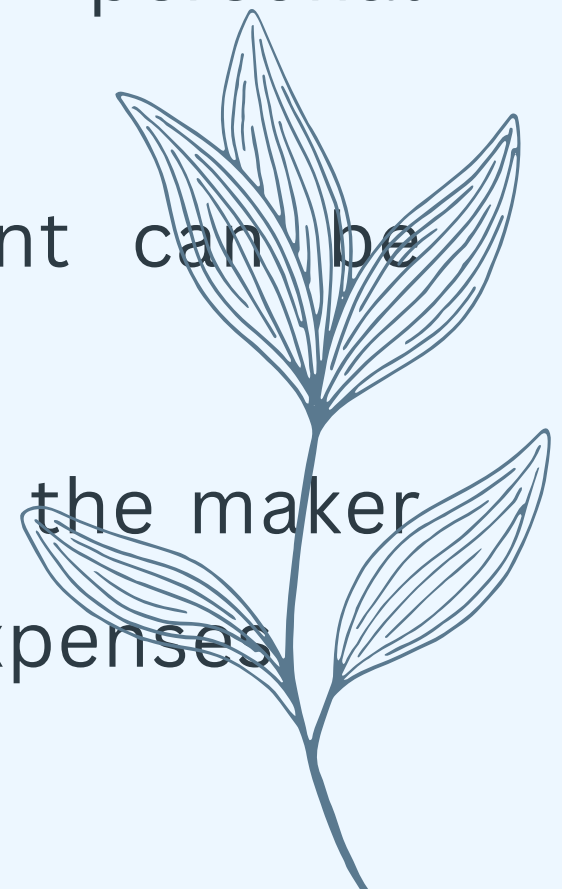
- (1) Statements, written or verbal, of relevant facts made by a person who is dead or who cannot be found, or who has become incapable of giving evidence, or whose attendance cannot be procured without an amount of delay or expense which under the circumstances of the case appears to the court unreasonable, are themselves relevant facts in the following cases:
- s.32 EA 1950 provides eight exceptions to relevant hearsay evidence
- s.32 EA 1950 is an general exception that subjects to specific provision such as s399 CPC.



Exception- s, 73A Evidence Act 1950



- This section facilitates the admissibility of both first hand hearsay and second hand hearsay.
- A document may be admitted as evidence of facts contained therein irrespective whether witness had personal knowledge of the contents of the documents.
- The testimony of the maker of the document can be dispensed with if such witness is not available.
- Court discretion to admit document even where the maker is available but it would cause undue delay and expenses.
- Safeguards to avoid abuse.



Exception- s,114A Evidence Act 1950



- This section has introduced a rebuttable presumption of fact applicable in both civil and criminal proceedings.
- Publication through the internet.
- admissibility of publication from the internet to establish identification and proof of the identity of an anonymous person involved in publication through internet.



Admissibility of Digital Evidence

Found or seized under
Criminal Procedure
Code

Documentary Evidence
vs

Oral Evidence

Relevancy Test.

no objection from
opponent

Rules of admissibility



SECTION 90A EVIDENCE ACT

1950

(1) In any criminal or civil proceeding a document produced by a computer, or a statement contained in such document, shall be admissible as evidence of any fact stated therein if the document was produced by the computer in the course of its ordinary use, whether or not the person tendering the same is the maker of such document or statement.



SECTION 90A EVIDENCE ACT

1950

(2) For the purposes of this section it may be proved that a document was produced by a computer in the course of its ordinary use by tendering to the court a certificate signed by a person who either before or after the production of the document by the computer is responsible for the management of the operation of that computer, or for the conduct of the activities for which that computer was used.



SECTION 90A EVIDENCE ACT

1950

(3)(a) It shall be sufficient, in a certificate given under subsection (2), for a matter to be stated to the best of the knowledge and belief of the person stating it.

(b) A certificate given under subsection (2) shall be admissible in evidence as prima facie proof of all matters stated in it without proof of signature of the person who gave the certificate.



SECTION 90A EVIDENCE ACT

1950

(4) Where a certificate is given under subsection (2), it shall be presumed that the computer referred to in the certificate was in good working order and was operating properly in all respects throughout the material part of the period during which the document was produced.



SECTION 90A EVIDENCE ACT

1950

(6) A document produced by a computer, or a statement contained in such document, shall be admissible in evidence whether or not it was produced by the computer after the commencement of the criminal or civil proceeding or after the commencement of any investigation or inquiry, in relation to the criminal or civil proceeding or such investigation or inquiry, and any document so produced by a computer shall be deemed to be produced by the computer in the course of its ordinary use.



SECTION 90A EVIDENCE ACT

1950

(7) Notwithstanding anything contained in this section, a document produced by a computer, or a statement contained in such document, shall not be admissible in evidence in any criminal proceeding, where it is given in evidence by or on behalf of the person who is charged with an offence in such proceeding the person so charged with the offence being a person who was-

(a) responsible for the management of the operation of that computer or for the conduct of the activities for which that computer was used; or

(b) in any manner or to any extent involved, directly or indirectly, in the production of the document by the computer.



SECTION 90B EVIDENCE ACT

1950

In estimating the weight, if any, to be attached to a document, or a statement contained in a document, admitted by virtue of section 90A, the court-

(a) may draw any reasonable inference from circumstances relating to the document or the statement, including the manner and purpose of its creation, or its accuracy or otherwise;

(b) shall have regard to-


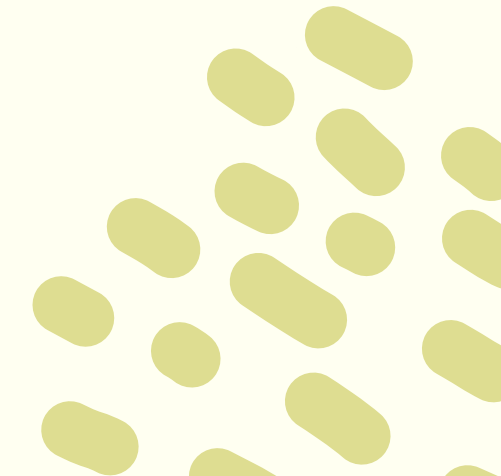
(i) the interval of time between the occurrence or existence of the facts stated in the document or statement, and the supply of the relevant information or matter into the computer; and

(ii) whether or not the person who supplies, or any person concerned with the supply of, such information or the custody of the document, or the document containing the statement, had any incentive to conceal or misrepresent all or any of the facts stated in the document or statement.





S.90B EVIDENCE ACT 1950

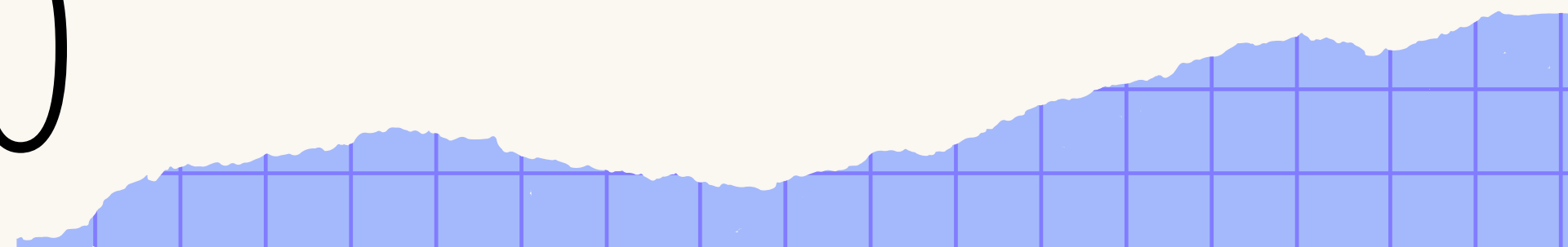
- 
- 
- dealt with the weight/probative value to be attached in a document/ statement contained in a document.
 - s 90B therefore distinguished between admissibility and the authenticity, reliability and integrity of the evidence.
 - Admissibility of the evidence as primary evidence is not synonymous with its authenticity.
 - Proof of evidence is governed by s.61 to s.78A Evidence Act 1950 which are capable of being applied to digital evidence.



Admissibility



DOES NOT PRESUME
AUTHENTICITY S90B
EA 1950



It was held in another American case, United States v Smith 918 F 2d 1501, 1510 that the 'government may authenticate a document solely through the use of circumstantial evidence including the document's own distinctive characteristics and the circumstances surrounding its discovery.

**PETROLEUM NASIONAL
BERHAD (PETRONAS) &
ORS v KHOO NEE KIONG
[2003] 4 MLJ 216 (HC)**

Similarly here, in my judgement, the plaintiffs can rely on circumstantial evidence to show that the defendant is the author and sender of the impugned statements contained in the e-mail and web page as the provisions of the Evidence Act 1952 in particular s 62, s 90A, s 90B, and s 3 which defines 'document' to include, inter alia, any electronic ... data whatsoever can be utilized for this purpose although there is no specific reference to e-mail or webpage or website.

SECTION 90C EVIDENCE ACT

1950

The provisions of sections 90A and 90B shall prevail and have full force and effect notwithstanding anything inconsistent therewith, or contrary thereto, contained in any other provision of this Act, or in the Bankers' Books (Evidence) Act 1949 [Act 33], or in any provision of any written law relating to certification, production or extraction of documents or in any rule of law or practice relating to production, admission, or proof, of evidence in any criminal or civil proceeding.



By Steven Chow

Challenges on the admissibility

“In Malaysia, digital evidence is admissible as documentary evidence and primary evidence. The admissibility of digital evidence is established under sections 90A, 90B and 90C of the Evidence Act 1950.

**Lim Peng Hock & Anor v
Chuah Peng San
(Peguambela &
Peguamcara, Pemilik
tunggal yang beramal
sebagai Tetuan Chuah,
Halim & Co) & Anor
[2021] MLJU 192 (COA)**

We cannot view it lightly as to this evidence because digital evidence is also very fragile and could easily be altered. Therefore the issues of authenticity and reliability are important for digital evidence.’

It was decided in the case of Gnanasegaran that there are two ways by which documents produced by computers are admitted as evidence in court. Firstly, by giving oral evidence that it was produced by a computer, or secondly, by producing a certificate under section 90A (2) EA..."

**Ahmad Najib
bin Aris v. PP
[2009] 2 CLJ
800 (FC)**



Digital Evidence of other nature

Electronic fingerprinting

- Hashing

01

CCTV Recordings

02

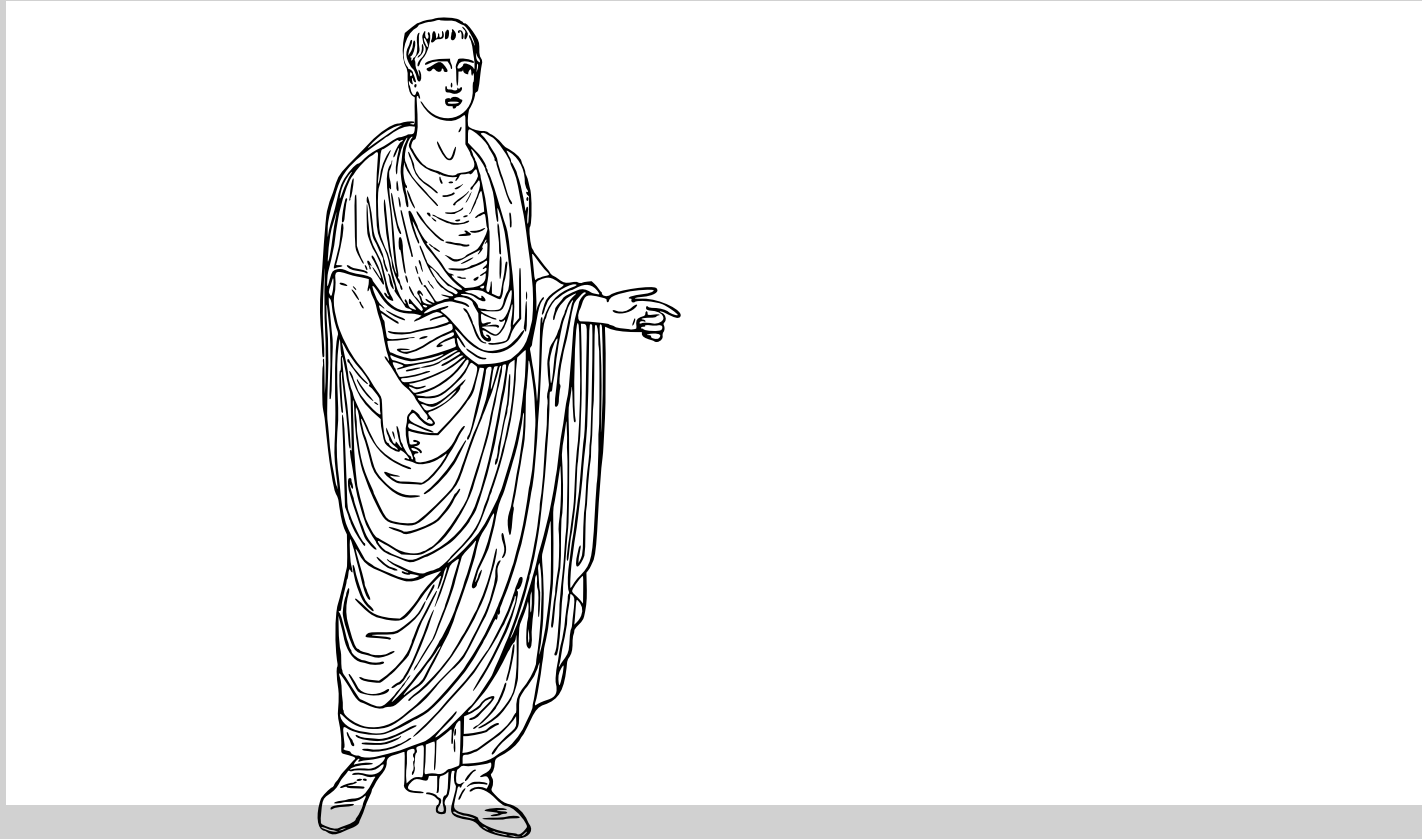
Whasapp Conversations

03

Emails

04

Facebook posting



Hashing

Method of Authentication

- Hash value is a unique numerical identifier that can be assigned to a file based in a standard mathematical algorithm applied to the data set.
- Hashing can be a mean of efficiency determine whether two files are exact duplicates. of each other or tweeter a single file has been altered.
- minimize the possibility of tampering.

“any digital file can be easily modified, tampered with. Therefore, the process of acquiring the digital evidence from the source must follow the forensic process to ensure the authenticity of the recording;”

**Pacific &
Orient
Insurance Co
Bhd v
Mohammad
Hafizi bin
Bahari & Anor
[2023] 11 MLJ
933 (HC)**

PP v Ramli
Shafie (2002) 6
MLJ 153 (HC)

“All the photographs had been properly identified by PW2, PW3 and PW4 as an accurate representation of what they depicted without any objection to their authenticity. As such they can be marked as exhibits. It has been held that although the usual method of proving the relevance of photographs will be by calling the photographer as a witness, this is not essential to their admissibility.”

“The document cannot be admitted without the maker being called if the authenticity of the document is disputed.”

**Asia
Cosmetics
Enterprise
Company
Limited V.
Mississippi
Global Sdn
Bhd [2022]
MLJU 451 (HC)**

“If, however, it is alleged that the tape has been tampered with, it would be proper to require the witness to give his recollection of the recorded conversation before the tape is played or he is allowed to refer to the transcript. Otherwise this is not necessary.”

**Mohd Ali
Jaafar v PP
[1998] 4 MLJ
210 (HC)**



“A CCTV tape is therefore a document produced by a computer. It follows that the CCTV tapes (P19A-D) must satisfy the requirements of s 90A of the Act before they can be admitted in evidence. As this had not been done they are inadmissible.”

**Ahmad Najib
Bin Aris V
Pendakwa
Raya [2009] 2
MLJ 613 (FC)**

**R v Maqsud
Ali [1965] 2 All
ER 464**

Evidence of things seen through telescopes or binoculars which otherwise could not be picked up by the naked eye have been admitted, and now there are devices for picking up, transmitting, and recording conversations. We see no difference in principle between a tape recording and a photograph. In saying this we must not be taken as saying that such recordings are admissible whatever the circumstances, but it does appear to this court wrong to deny to the law of evidence advantages to be gained by new techniques and new devices, provided the accuracy of the recording can be proved and the voices recorded properly identified; provided also that the evidence is relevant and otherwise admissible, we are satisfied that a tape recording is admissible in evidence.

**Lee Chor
Hean v
PP[2018] 1 LNS
2025 (HC)**

Real Evidence vs
Requirement under
section 90A Evidence Act
1950

We agreed that s. 399(i) CPC was not merely a procedural provision but it contained inter alia rules of admissibility of chemist report which dispensed with the need to call the Government chemist as maker of the document as a witness. The learned Counsel for the appellant also referred to the case of Chah Siew Kok v. PP[1987] CLJ 518 (Rep) where Peh Swee Chin J held that if a chemist report was admitted in contravention of s. 399 of the Criminal Procedure Code, it would be an irregularity of a serious nature and the report in such circumstances was inadmissible evidence despite its admission. He also held that a waiver or an estoppel could not be raised against s. 399 which imposed a duty on the prosecution to call the chemist as a witness. Further a waiver by an accused person could not be held against him in regard to rules of procedure and evidence in criminal proceedings.

**OOI LEAN CHAI v.
PUBLIC
PROSECUTOR[199
1] 1 CLJ Rep 337
(SC)**

Any admission of inadmissible evidence even with consent or by waiver of the accused was wrongful and such inadmissible evidence remained inadmissible evidence, the effect of which was open to any Court to assess.

**OOI LEAN
CHAI v.
PUBLIC
PROSECUTOR[
1991] 1 CLJ
Rep 337 (SC)**

(1) A trial judge in a criminal trial has always a discretion to refuse to admit evidence if in his opinion its prejudicial effect outweighs its probative value.

(2) Save with regard to admissions and confessions and generally with regard to evidence obtained from the accused after commission of the offence, he has no discretion to refuse to admit relevant admissible evidence on the ground that it was obtained by improper or unfair means. The court is not concerned with how it was obtained.

**Ramli Kechik
v. Public
Prosecutor
[1986] 1 CLJ
308. (SC)**

**HLC v. PTL &
ANOR [2024] 5
CLJ 117 (HC)**

In contrast, the current case lacked verification of the origin of the subject matter of the screenshots, namely the video calls and WhatsApp messages, with the respondent denying ownership or recognition of the phone or messages from which the screenshots were supposedly taken. Moreover, discrepancies such as a misspelled name purportedly belonging to the co-respondent on the contact page and the absence of timestamps on the WhatsApp messages further compromised the reliability of the screenshots.



The seven documents were secondary documents. The plaintiff had not shown the existence of any of the circumstances in s. 65 of the Act for the court to accept secondary documents as evidence. The plaintiff's reliance on the ROC was untenable as admissibility was governed under the Act. The ROC merely act as a guide to distinguish the various documents for ease of the proceedings; in no way does the ROC displace the Act on admissibility of documents. The condition precedent for the admissibility of documents, under s. 32 of the Act, had not been shown or satisfied in this case. The plaintiff's reliance on s. 73A of the Act was also misplaced as the provision only provides for dispensation of the attendance of a witness under certain conditions but subject to the original document being produced. In this case, the issue was not on the non-availability of the witness but rather, as to the admissibility of the documents.

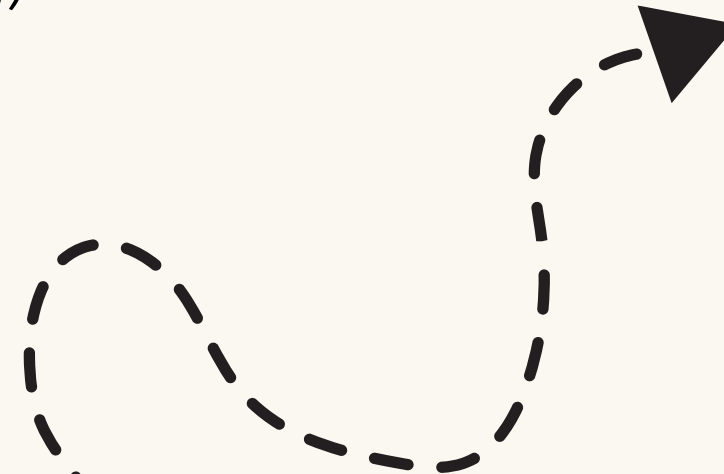
**TROY
INFORMATION
TECHNOLOGY
MALAYSIA SDN
BHD v. NISSEN
TECHNOLOGY SDN
BHD [2024] 5 CLJ
679 (HC)**

PRESERVATION

of Digital Evidence



- when a computer information is deleted, most computer system do not actually erase the information by rather mark as available for re-use.
- Absent of utility program.
- Backup software are only copying active files.
- Stop using the hard disk
- image or mirror copy of the hard disk.
- The doctrine of spoliation can result in court imposing penalty on a party that destroy or permits the destruction of relevant evidence.
- inference could be drawn that the party destroyed the evidence did so because it could have disclosed facts averse to that party case.
- s. 114(g) Evidence Act 1950.



Statutory preservation under National Archives Act 2003- Prohibition against destruction of Public Record

25. (1) Notwithstanding any written law to the contrary, no person shall, except with the prior written consent of the Director General, destroy or authorize the destruction of any public records which are in the custody or under the control of that person.

(2) A person intending to destroy or authorize the destruction of any public records shall-

(a) notify the Director General in the prescribed form of the intention to do so; and

(b) in such notification, specify the nature of the public records in question.

(3) The Director General may require any public records specified in a notification under subsection (2) to be made available to him for his inspection and he may inspect such records.

(4) The Director General may, in accordance with section 26, consent to the destruction of the public records specified in the notification under subsection (2).

(5) Any person who contravenes subsections (1) and (2) or who fails to have available any public record as required by the Director General under subsection (3) commits an offence and shall on conviction be liable to a fine not exceeding five thousand ringgit or to imprisonment for a term not exceeding one year or to both.

s.26 National Archives Act 2003- Disposal of Public Record

(1) The Director General may authorize the disposal of any public records or classes of public records which-

(a) by reason of their number, kind or routine nature, do not in his opinion possess any permanent and enduring national or historical value or both;

(b) are not required for reference purposes in any public office after-

(i) action on the public records are completed;

(ii) the expiration of such period as may be agreed upon between the Director General and the administrative head of that public office; or

(c) their physical condition does not permit their continued preservation.

s.42 National Archives Act 2003- Legal Validity of Photographic Copies and Extracts

- (1) In any legal proceedings, a microfilm recording and a photographic copy of or an extract from-
 - (a) any records in the custody or under the control of the National Archives; or
 - (b) any records or any part thereof which have been destroyed or otherwise disposed of from the custody or under the control of the National Archives, purporting to have been examined and certified as authentic by the Director General and to be sealed or stamped with the official seal of the Director General shall be admissible as evidence without any further or other proof thereof if the original records would have been admissible as evidence in those proceedings.
- (2) The court before which a microfilm recording, a photographic copy or an extract is tendered in evidence under subsection (1) may, if the original is in existence, require the production of the original and thereupon subsection (1) shall cease to apply to the recording, copy or extract.
- (3) For the purpose of this section, enlargement of microfilm recordings of records shall be deemed to be photographic copies of those records.

s.43 National Archives Act 2003- Authentication of Photographic Copies and Extracts

(1) Any microfilm recording, photographic copy or extract which the Director General is authorized or required under this Act to authenticate may be signed by the proper officer on behalf of the Director General and shall be sealed or stamped with the official seal of the Director General.

(2) Any microfilm recording, photographic copy or extract purporting to bear the signature of the proper officer and the official seal of the Director General shall, until the contrary is proved, be deemed to have been duly authenticated by the authority of the Director General.

(3) There shall be paid such fees as may be prescribed for the authentication under this section of any microfilm recording, photographic copy or extract on the application of any person.

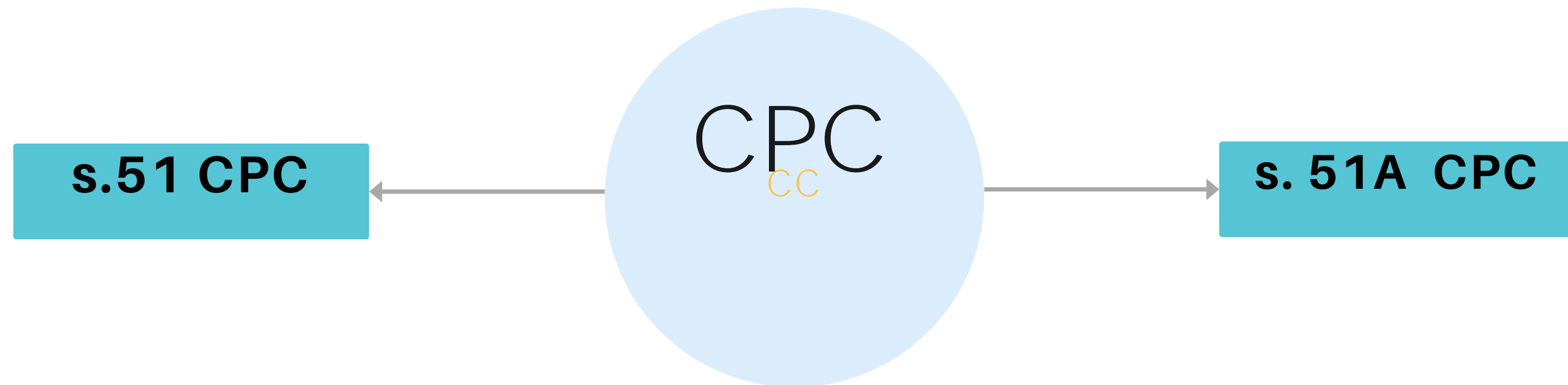
Illustration (g) of s. 114 of the Evidence Act, 1950 has grown over the years in terms of the volume of literature written on it. It refers to the presumption raised from wilful withholding of evidence and from spoliation particularly in regard to destruction, mutilation, suppression and fabrication of evidence.

Thus, if a man wrongfully withholds evidence, every presumption to his disadvantage consistent with the facts admitted or proved will of course be adopted.

To entitle the Court to draw an inference unfavourable to a party, the Court must be satisfied that the evidence was in existence and could be produced

**PUBLIC
PROSECUTOR
v. GAN
KWONG [1997]
2 CLJ SUPP 433**

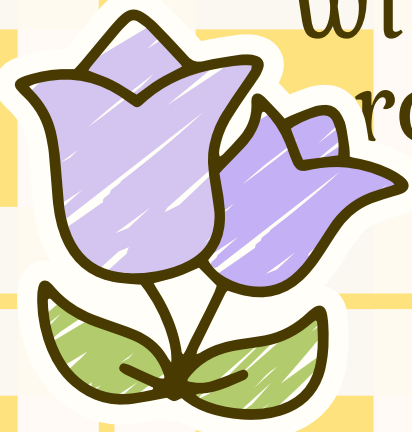
DISCOVERY IN CRIMINAL PROCEEDINGS



S 51 CPC

(1) Whenever any Court or police officer making a police investigation considers that the production of any property or document is necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding under this Code by or before that Court or officer, such Court may issue a summons or such officer a written order to the person in whose possession or power such property or document is believed to be requiring him to attend and produce it or to produce it at the time and place stated in the summons or order.

(2) Any person required under this section merely to produce any property or document shall be deemed to have complied with the requisition if he causes the property or document to be produced instead of attending personally to produce the same.



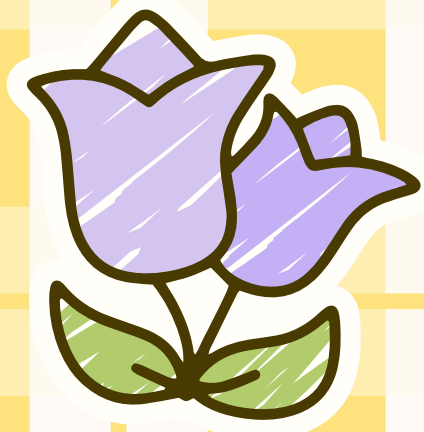
S 51A CPC

(1) The prosecution shall before the commencement of the trial deliver to the accused the following documents:

(a) a copy of the information made under section 107 relating to the commission of the offence to which the accused is charged, if any;

(b) a copy of any document which would be tendered as part of the evidence for the prosecution; and

(c) a written statement of facts favourable to the defence of the accused signed under the hand of the Public Prosecutor or any person conducting the prosecution.



Way Forward

- **Cryptocurrency**
- **AI**
- **Blockchain**
- **Other digital assets**
- **E- Discovery in Criminal Proceedings**
- **Cost of data recovery services**

