NATIONAL UNIVERSITY OF SINGAPORE

IFS 4101 – LEGAL ASPECTS OF INFORMATION SECURITY

AY2021/2022, Semester 2, Week 9

EVIDENCE AND INFORMATION SECURITY

REQUIRED READINGS FOR THE TOPIC

1. *Second Reading, Evidence (Amendment) Bill 2012*, Official reports – Parliamentary Debates (Hansard), Feb. 14, 2012, 1127, 1144.
2. *Roy S Selvarajah v PP* [1998] 3 SLR 517; [1998] SGHC 272, [38]-[50]
3. *Aw Kew Lim v. PP* [1987] SLR(R) 443, [1987] SGHC 33, [8]-[10]
4. *PP v. Ang Soon Huat* [1990] 2 SLR(R) 246; [1990] SGHC 121, [24]-[30]
5. *Mitfam International Ltd. v. Motley Resources Pte Ltd* [2014] 1 SLR 1253, [2013] SGHC 270, [1]-[6] (facts), [23]-[32]
6. *Telemedia Pacific Group v Credit Agricole* [2015] 1 SLR 338; [2014] SGHC 235, [242]- [262]
7. Wall Street Journal, How Morgan Stanley Botched a Big Case by Fumbling Emails, May 16, 2005 (Factiva).

1. INTRODUCTION

We have spent the last few weeks studying the types of substantive laws that an IS professional could encounter. These include laws that create rights (e.g., intellectual property laws) and laws that require citizens to refrain from engaging in behaviour that are unacceptable to society (e.g., criminal laws).

Whenever a case is brought before the court concerning one of these substantive laws, the parties to the case (plaintiff and defendant in a civil case, and prosecutor and defendant in a criminal case) will present its case to the court. In presenting its case, the plaintiff or prosecutor will claim that a wrong occurred based on a set of events, while the defendant will deny the that the events occurred or that a wrong happened.

These claims about the existence or absence of stated events must be sifted and weighed for their probity. In the common law system, rules have been developed that the courts use to decide if claims should be entertained (i.e., admitted into evidence), and which ones should be ignored. These rules are encapsulated in what is known as the laws or rules of evidence.

Why should the IS professional care about the rules of evidence? The obvious answer lies in the "Integrity" portion of the confidentiality-integrity-availability triad. It is the IS professionals' job to ensure the preservation of data integrity in a manner that will allow that data to be used as evidence in court proceedings. Systems and access controls must be designed in such a manner to assure the court that the evidence that is submitted is trustworthy. If the systems and the manner in which data is managed in an information system is not properly designed and implemented to collect accurate data, preserve evidence and prevent spoliation of evidence during litigation, the design and

implementation failure can cause a party to lose its case in court because that information will be excluded from consideration by the court in making its decision.

2. WHAT ARE THE RULES OF EVIDENCE?

Rules of evidence are the rules that tell us how facts are to be proven in a legal proceeding. These rules are used to determine:

- The category or type of evidence can be submitted to the trier of fact for use in making a decision about the case (admit into evidence).
- The weight that is to be attributed to that evidence during decision-making (weight of evidence).
- The methods by which the evidence must be produced.
- The party that bears the responsibility to produce the evidence (burden of proof).
- The amount of evidence that needs to be produced in order to prove the claim (standard of proof).

For this course, our study will focus on the first bullet point – i.e., the rules that determine what category or type of evidence can be considered by the body that decides the outcome of the trial (judge(s) and, in places like the US and UK, the jury). We say that such evidence is "admissible" and the rules are described as the "rules of admissibility".

The following principles stand behind rules that have been developed to determine when evidence is admissible:

- Evidence must be relevant;
- Evidence must be reliable; and
- Evidence must be fairly admitted.

a. Relevance: Inclusionary vs. Exclusionary Rules of Evidence

The complicated rules governing the use of evidence at trial is a unique feature of the common law world where, historically, trials are judged by a jury (also known as the trier of fact). To constitute a jury necessarily means that the court must take people out of their normal routine to sit through a trial, which also means that operationally, the system must force a trial to be decided within a time-bound period. As a result, the process of discovery of the truth becomes a highly stage-managed affair, with complicated protocols to make sure that the evidence that is admitted reaches a minimum standard that the layman can use to form his decision. In contrast, in a civil law system, the trial judge also acts as the inquisitor and is trusted to figure out which evidence should be considered, and which should be excluded in the judge's decision-making process. As a result, the rules of evidence become a much less complicated affair as the judge gets to decide what she finds to be acceptable evidence.

Within the common law jurisdiction, including England, the vast majority operate on the basis that evidence is admissible if it tends to show the existence or non-existence of any fact in issue. The is no rule or law mandating the judges to accept any item of information into evidence. However, there are rules that instruct the judges how to identify evidence that is not admissible. The judges are also free to exclude any evidence that have been determined to not make any impact on the case. In these jurisdictions, the rules of evidence contain "exclusionary" rules of admissibility.

The situation in Singapore is somewhat different. Sir James Fitzjames Stephen's Indian Evidence Act of 1872 ("IEA") governs the law of evidence in Singapore and almost a dozen other common law jurisdictions. But the fundamental features of the IEA would undoubtedly be considered anomalous when viewed against modern notions of relevance and admissibility in that the IEA represents an attempt to define what constitutes "relevant" evidence in an exhaustive manner, instead of an exclusionary manner. This type of rules are called "inclusionary" rules of evidence. In an inclusionary system, the judges can't exercise discretion to ignore evidence if the evidence is within the scope of admissible evidence as defined in the IEA. Similarly, evidence that falls outside the scope of the IEA cannot be admitted into evidence even though it may show the existence or non-existence of any fact in issue. However, the judge can exclude evidence in some situations. See Section C.

As Sir James stated in the introduction to the IEA:

> *"In the preceding pages I have stated and illustrated the theory of judicial evidence on which the Evidence Act is based. I have but little to add to that explanation. The **Act speaks for itself**. No labour was spared to make its provisions complete and distinct. As the first section **repeals all unwritten rules of evidence**, and as the Act itself supplies a distinct body of law upon the subject, its object would be defeated by elaborate references to English cases. In so far as it is obscure or incomplete, the judges and the Legislature are its proper critics. If it is turned into an abridgment of the law which it was meant to replace, it will be injurious instead of being useful to those for whom it was intended."*

(Emphasis added.)

In the chapter Singapore, of the book, Electronic Evidence (Stephen Mason ed., 2012) (Chapter 17), authors Daniel Sng and Bryan Tan state:

> *In Singapore, evidence is only admissible in all judicial proceedings pursuant to the rules of evidence in the Singapore Evidence Act[1] and in other rules of evidence contained in any written law.[2] While learned academic writings exist that suggest that the Evidence Act is little more than a codification of the English laws of evidence,[3] the Privy Council has authoritatively pronounced the Evidence Act to be a codifying act.[4] The result is that although reference can be made to the English common law to aid in the interpretation of ambiguous rules in the Evidence Act,[5] where any part of evidence law is expressly dealt with by the Evidence Act, the courts must give effect to the relevant provisions of the Evidence Act regardless of whether they differ from the common law rule of evidence.[6]*

---

[1] Cap 97, 1997 Rev Ed.
[2] Section 2(2) of the Evidence Act states that "[a]ll rules of evidence not contained in any written law, so far as such rules are inconsistent with any of the provisions of this Act, are repealed."
[3] James Fitzjames Stephen, *The Indian Evidence Act with an Introduction on the Principles of Judicial Evidence* 2 (Thacker, Spink & Co, 1872) [hereinafter *An Introduction to the Indian Evidence Act*].
[4] *Mohamed Syedol Ariffin v Yeoh Ooi Gark* [1916] 2 A.C. 575; *Jayasena v R* [1970] AC 618; *Public Prosecutor v Yuvaraj* [1969] 2 MLJ 89, 90 per Lord Diplock.
[5] *Saminathan & Ors v Public Prosecutor* [1955] MLJ 121, 124.
[6] *Public Prosecutor v Yuvaraj* [1969] 2 MLJ 89, 90 per Lord Diplock. An English rule or principle cannot be accepted if it will thereby vary the true and actual meaning of the provision in the Evidence Act, or it will deny the provision in the Evidence Act any effect: *Mohamed Syedol Ariffin v Yeoh Ooi Gark* (*ibid*) at 580 per Lord Shaw of Dunfermline.

Questions:

1. Based on the above, please explain the difference in the legal regime for admitting evidence in Singapore versus England.

2. What did Sir James mean when he said that the "Act speaks for itself" in the introduction to the IEA?

b. Relevance: What constitutes relevant/admissible evidence?

The fact that Singapore's rules of evidence are inclusionary has significant impact in the type of data that needs to be gathered and the evidence that can be presented to a Singapore court. The following passage explains this difference:

> *The Evidence Act defines a fact as relevant "when the one is connected with the other in any of the ways referred to in the provisions of this Act relating to the relevancy of facts."*[7] *This definition collapses the evidential distinction between "relevance" as referring to logical relevance – where "according to the common course of events one [fact] either taken by itself or in connection with other facts proves or renders probable the past, present, or future existence or non-existence of the other [fact]"*[8] *– and legal relevance or rules of admissibility, which at the common law are rules which exclude relevant evidence for legal or policy reasons unless such evidence falls within one of the four general exceptions to these*[9] *exclusionary rules – hearsay, opinion, character and conduct on other occasions. James Fitzjames Stephen, the draftsman for the Indian Evidence Act (the predecessor act to the Singapore Evidence Act) thus sought to state all the "admissibility" rules of evidence in their affirmative form, in Part I of the Evidence Act. Although an item of evidence can be "relevant"*[10] *under different relevancy provisions in the Evidence Act, of evidence that cannot be rendered "relevant" under any of the provisions of the Evidence Act is inadmissible.*

Because of the way that Singapore's Evidence Act is set up, when considering what type of records to produce during litigation, the first point of reference is the Evidence Act, not whether or not that record has connection to the facts in issue. The Evidence Act in Singapore is a **self-contained code** that fuses the concepts of logical and legal relevancy.

The Evidence Act describes the following evidence as being admissible:

- existence or non-existence of facts in issue and relevant facts: s 5
- facts forming part of the same transaction as a fact in issue: s 6
- facts which are the occasion, cause or effect of facts in issue or relevant facts: s 7
- facts which show or constitute a motive or preparation for any fact in issue or relevant fact, and previous or subsequent conduct, influenced or is influenced by any fact in issue or relevant fact: s 8
- facts necessary to explain or introduce relevant facts: s 9
- things said or done by conspirator in reference to common design: s 10

---

[7] Section 3(2), Evidence Act.
[8] James Fitzjames Stephen, *A Digest of The Law of Evidence* 4 (London, 1886).
[9] *Id*, at xii. *See also* Wigmore, *Evidence in Trials at Common Law* §10 (Tillers rev. 1988), at 667.
[10] *An Introduction to the Indian Evidence Act*, at 55.

- facts inconsistent with any fact in issue or relevant fact, or by themselves or in connection with other facts, make the existence or non-existence of any fact in issue or relevant fact highly probable or improbable: s 11

c. Do judges have any discretion in admitting evidence or disallowing evidence?

Even though the rules for admitting evidence are spelt out in the Evidence Act, the judge retains a discretion to disallow such evidence, if its admissibility would operate unfairly against the accused.[11] Examples of these will be where the evidence is unlawfully obtained, or obtained in circumstances that amounted to inducing the commission of an offence.[12] Although the Court of Appeal has denied that there is a defence of entrapment in Singapore,[13] there are also judicial pronouncements where the court has excluded the evidence obtained from the illegal conduct of a private investigation.[14] No distinction appears to be drawn between illegal conduct of a public investigation such as that by the police, and the illegal conduct of a private investigation. In both cases, the court will not sanction the illegal conduct by admitting the evidence.[15]

d. What forms do evidence take?

Evidence can be characterized according to the physical form of the evidence. In this characterization, there are three main forms in which evidence can take: oral evidence, documentary evidence and real evidence.

Oral evidence is in the form of witnesses' testimonies about matters for which they have knowledge. A witness must first be "competent" before he can give oral evidence. The oral testimony of the witness can be delivered in oral form in court after the witness is first sworn, or it can be in attested written form (affidavits). Oral evidence can also be obtained by way of a subpoena (an order that a person attend court). Oral testimony will be examined in a court of law. The examination of a witness by the party who calls the witness is known as the examination in chief. The examination by the opposing party is known as cross-examination. The duty of a witness is to answer questions posed by the plaintiff's lawyer, the defendant's lawyer and the judge honestly and to the best of his or her knowledge.

Documentary evidence takes the form of records of matters in question. These could be business books, computer logs, or even records of oral statements. Documents tendered in evidence can be inspected by both parties and challenged. The process by which documents in relevant to the action are found is known as "discovery". The background to the documents also has to be established before they can be admitted, a process known as "authentication". More detailed discussion of these will follow.

Real evidence refers to tangible items that relate to the matters in question. For instance, the murder weapon is "real evidence". The powder which is alleged to have been trafficked as a "controlled substance" is "real evidence". Real evidence also refers to contemporaneous records (as opposed to "after-the-fact" or documentary records) of the event or incident in question. Because "real evidence" is so persuasive, the key rule as to the admissibility of "real evidence" is its "authentication" or lack of authentication.

---

[11] *Cheng Swee Tiang v PP* [1964] MLJ 291(Court of Appeal, Singapore).
[12] *See e.g. Ajmer Singh v PP* [1986] SLR 454) (High Court, Singapore).
[13] *How Poh Sun v PP* [1991] 2 SLR(R) 270 (Court of Appeal, Singapore).
[14] *SM Summit Holdings Ltd v PP* [1997] 3 SLR 922 (High Court, Singapore).
[15] *Wong Keng Leong Rayney v Law Society of Singapore* [2006] 4 SLR(R) 934 (High Court, Singapore).

3. WHAT IS ELECTRONIC EVIDENCE?

Review the version of the Evidence Act before the 2012 amendments. You will find that there was a special section on electronic evidence in the Evidence Act. These were removed in 2012.

See Second Reading, Evidence (Amendment) Bill 2012, Official reports – Parliamentary Debates (Hansard), Feb. 14, 2012, 1127, 1144.

The only reference that remains as to electronic evidence is that of an "electronic record" in s 3(1) and a reference to electronic records in s 9 and s 116A.

> S 3(1), Evidence Act (Cap 97, 1997 Rev Ed) (post-2012 amendments)
>
> **Interpretation**
>
> "electronic record" means a record generated, communicated, received or stored by electronic, magnetic, optical or other means in an information system or transmitted from one information system to another;

Questions:

1. Why was the pre-2012 Evidence Act not "electronic evidence" agnostic?

2. What changed between 2003 and 2021? Why?

4. WHAT IS THE RULE AGAINST HEARSAY?

Arguably the most important rule in evidence, and the rule which has the widest practical impact, is the rule against hearsay. The rule against hearsay is defined in the classic decision of *Subramaniam v PP* as follows:

> *"Evidence of a statement made to a witness by a person who is not himself called as a witness may or may not be hearsay. It is hearsay and inadmissible when the object of the evidence is to establish the truth of what is contained in the statement. It is not hearsay and is admissible when it is proposed to establish by the evidence, not the truth of the statement, but the fact that it was made. The fact that the statement was made, quite apart from its truth, is frequently relevant in considering the mental state and conduct thereafter of the witness or of some other person in whose presence the statement was made."*

Subramaniam v PP [1956] WLR 965 (Privy Council on appeal from Malaya) (ICLR).

The rationale behind this is that where a statement is made by a person who is not called as a witness, the veracity or accuracy of that statement cannot be questioned or challenged in court. However, some have challenged this rule on the basis that in Singapore, all our trials are by the judge and as legal professionals, they can be trusted to give the correct weight to hearsay statements. Nonetheless, the view that is taken is that the hearsay rule ensures that the best and most reliable evidence can be given, and that only limited exceptions to this rule are recognised. This is the position in Singapore law after the 2012 amendments.

The application of the rule against hearsay however requires some fine and difficult distinctions to be drawn.

Consider the following statements. Which of them constitute hearsay?

1. Andrew was charged with the offence of possessing ammunition to help terrorists. The offence carries the death sentence. Andrew pleaded the defence of duress. Andrew testified that: "*The terrorists threatened to kill me if I did not comply.*" Andrew also wants to admit into evidence the conversations he had with the terrorists.

2. Andrew was charged with murdering Victoria. Victoria's mother sought to testify that, "Victoria called me and told me that Andrew left her in the car at Exit 8 of the ECP to look for a public phone but he was going to find her once he called the tow truck company."

3. Victoria left a will stating that she bequeathed $2,000,000 to her godsons. Andrew wanted to claim under Victoria's will as Victoria's godson. Andrew seeks to admit into evidence the following statement: "Everyone knows I'm Victoria's godson. She called me "Godson" in front of all our friends."

4. As in Point 3, but Andrew wants to introduce an Ang Pow that he received from Victoria into evidence. The words "To My Godson" are on the Ang Pow.

5. As in Point 3, but Andrew wants to submit into evidence a Facebook video posting of Chinese New Year festivities where he was warmly seen to greet Victor as "my godma" and receiving Victoria's greeting as "my godson."

a. Negative hearsay

We have discussed the difficulties with establishing what constitutes hearsay. What if someone proffers the lack of a statement, or silence, to prove a certain point? E.g., no one ever complained about a particular latch being dangerous for the last 50 years and the design has never changed.

Consider the case of *Roy S Selvarajah v PP* [1998] 3 SLR 517; [1998] SGHC 272, [38]-[50]. What are the difficulties of dealing with the admissibility of "negative hearsay"? How are they compounded by the existence of electronic records? What are the facts in this case? Did the court in *Selvarajah* apply the evidence rules correctly? What would you as an information security professional have advised the Work Permit Department to do?

b. Electronic evidence as real evidence and as hearsay

Real evidence, for obvious reasons, are not treated as hearsay. A dead body speaks for itself. A damaged property speaks for itself. The white powder speaks for itself. The damaged $40,000 diamond-studded diary speaks for itself Contrast this, however, with the content contained within the damaged diary that you want to use to show that someone was present or not present at an event, which would constitute hearsay unless you can show that it was a contemporaneous recording.

Can you articulate for yourself the difference between real evidence and hearsay evidence? *See* Pinsler, *Evidence and the Litigation Process* (5th ed., 2015), 146-151 for an in-depth explanation.

It turns out that computer output can constitute hearsay or real evidence depending on how that output was produced. See Daniel Seng and Srirak Chakravarthi, *Computer Output as Evidence Consultation Pa*per (Sept. 2003), Technology Law Development

Group, Singapore Academy of Law, 85-92 [LINK]. Hence, we end up with complicated outcomes in cases that appear, at first blush, to be similar in their nature.

Questions:

Compare *Aw Kew Lim v. PP* [1987] SLR(R) 443, [1987] SGHC 33, [8]-[10] and *PP v. Ang Soon Huat* [1990] 2 SLR(R) 246; [1990] SGHC 121, [24]-[30] and ask yourself:

1. What evidence is (a) hearsay, or (b) real evidence) in each case? What is the basis for the distinction? Do you agree?

2. From an information security perspective, what can you do to facilitate the admissibility of electronic evidence as real evidence?

c. Exceptions to the hearsay rule

Notwithstanding the rule against hearsay, hearsay evidence is admitted in evidence nonetheless, because it is often the best, if not the only, evidence that is available. The rules that provide for the admission of hearsay evidence are known as hearsay exceptions.

The hearsay exception rules are found primarily in s 32 of the Evidence Act. For purposes of the information security course, four exceptions are the most pertinent. You should read and understand them. They are:

- the business records exception: s 32(b)
- the adverse statement exception: s 32(c)
- the unavailable witness exception: s 32(j)
- the admission by agreement exception: s 32(k)

Even though the operation of the hearsay rule allows for statements which are otherwise inadmissible to be admitted, the court may nonetheless give very little weight to the evidence.

Questions:

See *Gimpex Ltd v. Unity Holdings Business Ltd* [2015] 2 SLR 686; [2015] SGCA 8.

1. What was the evidence in question that was sought to be admitted under s 32 in Gimpex?

2. Which exception was applied?

3. What was the weight given to the evidence? Why?

5. AUTHENTICATION AND ADMITTING COMPUTER OUTPUT (POST-2012)

a. Authentication

There were many things that were not desirable under the pre-2012 system for admitting electronic evidence in Singapore. These were reviewed in two papers produced by the Technology Law Development Group of the Singapore Academy of Law in 2003 and 2004 ("TLDG"). *See* Daniel Seng and Srirak Chakravarthi, *Computer Output as Evidence Consultation Paper* (Sept. 2003), Technology Law Development Group, Singapore Academy of Law, 92-113 [LINK].

Questions:

1. What was the problem with the pre-2012 legal system as it then existed?
2. What was the proposal of the TLDG paper in 2003?

Section 32 of the Evidence Act, adopted as part of the 2012 amendments is reproduced below.

S 32, Evidence Act (Cap 97, 1997 Rev Ed) (post-2012 amendments)

Facts necessary to explain or introduce relevant facts

9. Facts necessary to explain or introduce a fact in issue or relevant fact, or which support or rebut an inference suggested by a fact in issue or relevant fact, or which establish the identity of any thing or person whose identity is relevant, or fix the time or place at which any fact in issue or relevant fact happened or which show the relation of parties by whom any such fact was transacted, are relevant in so far as they are necessary for that purpose.

Illustrations

(g) A seeks to adduce evidence against B in the form of an electronic record. The method and manner in which the electronic record was (properly or improperly) generated, communicated, received or stored (by A or B), the reliability of the devices and the circumstances in which the devices were (properly or improperly) used or operated to generate, communicate, receive or store the electronic record, may be relevant facts (if the contents are relevant) as authenticating the electronic record and therefore as explaining or introducing the electronic record, or identifying it as the relevant electronic record to support a finding that the record is, or is not, what its proponent A claims.

[Act 4 of 2012 wef 01/08/2012]

Questions:

As an information security professional, enumerate the different aspects of an item of electronic evidence for which a party has to "explain or introduce" as authentication evidence to support the admission of the electronic evidence

The observations in this paper formed the legal basis for the 2012 changes to the Evidence Act. The authors of the paper noted that the correct focus of the courts should be on authenticating the electronic evidence, regardless of whether it was real evidence or admissible hearsay.

This is best illustrated by the following case about electronic ledgers. *See Mitfam International Ltd. v. Motley Resources Pte Ltd* [2014] 1 SLR 1253, [2013] SGHC 270, [1]-[6] (facts), [23]-[32].

Questions:

Consider *Mitfam*.

1. What were the facts?
2. What did the defendant try to prove with the electronic ledgers?
3. Why did the defendant not succeed?
4. As an information security professional, how would you have tried to establish the case for the defendant?

b. Facilitative Presumptions

There were concerns by the TLDG authors that the abolition of the formalistic rules in the Evidence Act will discourage parties from relying on electronic evidence in court, or lead courts to frame the issues for authentication of electronic evidence erroneously.

Questions:

1. How would issues of authentication be dealt with under the post-2012 Evidence Act regime?
2. How do the presumptions that courts are supposed to give to electronic records (see S 116A of the Evidence Act) assist in resolving issues with authentication? A copy of Section 116A of the Evidence Act is reproduced below.

S 116A, Evidence Act (Cap 97, 1997 Rev Ed) (post-2012 amendments)

Presumptions in relation to electronic records

116A.—(1) Unless evidence sufficient to raise doubt about the presumption is adduced, where a device or process is one that, or is of a kind that, if properly used, ordinarily produces or accurately communicates an electronic record, the court shall presume that in producing or communicating that electronic record on the occasion in question, the device or process produced or accurately communicated the electronic record.

Illustration

A seeks to adduce evidence in the form of an electronic record or document produced by an electronic device or process. A proves that the electronic device or process in question is one that, or is of a kind that, if properly used, ordinarily produces that electronic record or document. This is a relevant fact for the court to

presume that in producing the electronic record or document on the occasion in question, the electronic device or process produced the electronic record or document which A seeks to adduce.

(2) Unless evidence to the contrary is adduced, the court shall presume that any electronic record generated, recorded or stored is authentic if it is established that the electronic record was generated, recorded or stored in the usual and ordinary course of business by a person who was not a party to the proceedings on the occasion in question and who did not generate, record or store it under the control of the party seeking to introduce the electronic record.

Illustration

A seeks to adduce evidence against B in the form of an electronic record. The fact that the electronic record was generated, recorded or stored in the usual and ordinary course of business by C, a neutral third party, is a relevant fact for the court to presume that the electronic record is authentic.

(3) Unless evidence to the contrary is adduced, where an electronic record was generated, recorded or stored by a party who is adverse in interest to the party seeking to adduce the evidence, the court shall presume that the electronic record is authentic in relation to the authentication issues arising from the generation, recording or storage of that electronic record.

Illustration

A seeks to adduce evidence against B in the form of an electronic record. The fact that the electronic record was generated, recorded or stored by B, who opposes the relevance of the evidence, is a relevant fact for the court to presume that the electronic record is authentic. (4) For the purposes of subsection (2), in criminal proceedings a party to the proceedings shall include —

(a) the police officer or other officer of a law enforcement agency who was involved in the investigation of offences allegedly committed by the accused person; or

(b) an accomplice of the accused person even though he is not charged with an offence in the same proceedings.

(5) The Minister may make regulations providing for a process by which a document may be recorded or stored through the use of an imaging system, including providing for the appointment of one or more persons or organisations to certify these systems and their use, and for any matters incidental thereto, and an "approved process" in subsection (6) means a process that has been approved in accordance with the provisions of such regulations.

(6) Where an electronic record was recorded or stored from a document produced pursuant to an approved process, the court

shall presume, unless evidence to the contrary is adduced, that the electronic record accurately reproduces that document.

(7) The matters referred to in this section may be established by an affidavit given to the best of the deponent's knowledge and belief.

Questions:

Consider Telemedia Pacific Group v. Credit Agricole, [2015] 1 SLR 338; [2014] SGHC 235, [242]-[262].

1. What were the electronic records in issue in this case? Why did Credit Agricole succeed in relying on the Section 116A(1) presumption for its electronic records?

2. How would you handle these scenarios under the new post-2012 Evidence Act regime:

    a. Electronic files reconstructed by forensic specialist from deleted file fragments.
    b. Electronic files that have been tampered with.
    c. Fabricated electronic documents.
    d. Impersonated online communications.

6. BEST EVIDENCE RULE

The ""best evidence" rule in rules of evidence is a legal principle that seeks to uphold the original copy of a document as evidence superior to any other kind of evidence. In other words, secondary evidence, in the form of a copy of the original document, is inadmissible if the original can be found. However, the concept of an "original document" is an unnecessary one in the context of electronic evidence. To this end, the best evidence rule for computer output under s 36 was also removed and assimilated into the existing best evidence rule in ss 64 and 65 of the Evidence Act. The rule is that whether electronic evidence is "best evidence" or not depends on whether it is "manifestly or consistently acted on" as reflecting the document accurately.

Ss 3(1), 64, 65, Evidence Act (Cap 97, 1997 Rev Ed) (post-2012 amendments)

Interpretation

"copy of a document" includes —

(a) in the case of a document falling within paragraph (d) but not paragraph (e) of the definition of "document", a transcript of the sounds or other data embodied in it; (b) in the case of a document falling within paragraph (e) but not paragraph (d) of that definition, a reproduction or still reproduction of the image or images embodied in it, whether enlarged or not;

(c) in the case of a document falling within paragraphs (d) and (e) of that definition, such a transcript together with such a still reproduction; and

(d) in the case of a document not falling within paragraph (e) of that definition of which a visual image is embodied in a document falling within that paragraph, a reproduction of that image, whether enlarged or not, and any reference to a copy of the material part of a document must be construed accordingly;

"document" includes, in addition to a document in writing —

(a) any map, plan, graph or drawing;

11

(b) any photograph;

(c) any label, marking or other writing which identifies or describes anything of

which it forms a part, or to which it is attached by any means whatsoever;

(d) any disc, tape, sound-track or other device in which sounds or other data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom;

(e) any film (including microfilm), negative, tape, disc or other device in which one or more visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom; and

(f) any paper or other material on which there are marks, impressions, figures, letters, symbols or perforations having a meaning for persons qualified to interpret them;

Primary evidence

64. Primary evidence means the document itself produced for the inspection of the court. Explanation 3.—Notwithstanding 2, if a copy of a document in the form of an electronic record is shown to reflect that document accurately, then the copy is primary evidence.

Illustrations

(a) An electronic record, which has been manifestly or consistently acted on, relied upon, or used as the information recorded or stored on the computer system (the document), is primary evidence of that document.

(b) If the electronic record has not been manifestly or consistently acted on, relied upon, or used as a record of the information in the document, the electronic record may be a copy of the document and treated as secondary evidence of that document.

7. ELECTRONIC DISCOVERY

a. Discovery in civil proceedings

Discovery refers to the phase of the process of civil litigation where parties are given a chance to inspect each other's documentary evidence.[16] The rules allow for this because of the nature of the common law trial – it is timebound and must be completed during some set time when the jury will be available. Therefore, to ensure that there can be no danger of a "surprise" sprung at the last minute, the common law jurisdictions have established elaborate mechanisms for ensuring that each side shares all of its supporting evidence (including evidence that is adverse to one's own case or that support the other side's case) with the other ahead of the trial so that issues can be simplified.[17] The process frequently encourages the parties to enter into settlement as evidence that is adverse to one's case will frequently be produced by the other side.

Previously, a chance to inspect each other's documentary evidence was automatic. However, recent amendments to the Rules of Court require the parties seeking to discover the other party's documents to first make an application to the court.[18]

Where the documents in question are electronically stored documents, the parties may by *mutual agreement* or through *a court order* require that the electronically stored documents are discovered via a slightly different process. Special rules found in the Supreme Court Practice Directions spell out the revised processes. *See* Singapore Supreme Court Practice Directions 2015, Part V [LINK].

In particular, the following electronically stored documents (and their contents) may be discovered:

- electronic documents stored in various locations, media and recording devices, including folders or directories where the files are deleted, or in unallocated file spaces
- metadata about electronic documents
- documents which have to be subject to a "forensic inspection", which would include a forensic examination of the deleted files and unallocated file spaces

Any such electronic document which "are, or have been" within a party's "possession, custody or power" may be discoverable.[19]

In electronic discovery, parties are encouraged to collaborate and agree to the following matters, in an "electronic discovery plan":

- the scope and/or limits on documents to be given in discovery (including internal document metadata which is also discoverable[20])
- whether parties are prepared to make voluntary disclosures
- whether specific documents/classes of documents ought to be specifically preserved
- search terms to be used in reasonable searches (for a class of documents described by the search term[21]):

---

[16] Rules of Court, Order 24 [LINK].
[17] Rules of Court, O. 24, r.1(2).
[18] Rules of Court, O. 24, r.1.
[19] Rules of Court, O. 24, r.1(1).
[20] P.D., Part V. para 46.
[21] P.D., Part V, para 47.

- the search terms have to have at least two limits – the custodian/repository (who has the documents/where are the documents) and the search duration (when were the documents created, received or modified)[22]
- the searches shall not extend to documents which are not reasonably accessible, and have to be proportional and economical[23]
- whether preliminary searches and/or data sampling are to be conducted
- whether discovery is given in stages the name and format of discoverable documents[24]

The details are spelt out in Appendix E, Part 1 checklist in the Practice Directions.

Where the parties do not agree and a discovery order has to be made, the court will only make an electronic discovery order where it is proportional and economical to do so, given the number of electronic documents involved, the nature and complexity of the case, the value of the claim and financial position of each party, the ease and expense of retrieval of any particular document or class of documents, their availability and the relevance and materiality of the documents likely to be located.[25]

Unlike physical discovery, a party in electronic discovery may be exempted from having to list the documents discoverable. Instead, all that is required is to provide a category of documents and a meaningful description for each category of documents, including a claim that certain documents are privileged from production.[26] The list of documents itself must also be provided in an electronic, text searchable and structured format.[27]

After these documents have been discovered, the party seeking discovery may seek to inspect them, or be supplied copies of them (with their metadata) in lieu of inspection.[28] The party required to produce the documents must provide reasonable means and assistance to the party seeking discovery.[29] Special rules are provided for the inspection of computer databases, to ensure that the party entitled to inspection has access only to the records that are necessary, and is not allowed to trawl through the entire database.[30]

There is a lot of pressure on the solicitor or expert representing the party giving discovery from ensuring that privilege over privileged documents are asserted,[31] and/or are not inspected.[32] Even though there are restrictions on the use inadvertently disclosed privileged documents[33], the party's case can still be significantly compromised as the other party may seek to exploit the information indirectly and for tactical advantage.

Applications for forensic inspections can only be sought after discovery of the electronic medium or recording device has been given.[34] See the Wall Street Journal article (required reading #7) to understand how electronic discovery can cause even the biggest companies to fall.

---

[22] P.D., Part V, para 47(1).
[23] P.D., Part V, para 47(2).
[24] P.D., Part V, para 47(2).
[25] P.D., Part V, para. 48.
[26] P.D., Part V, para. 53(2)(e).
[27] P.D., Part V, para. 59(6).
[28] Rules of Court, O.24, r.10; P.D., Part V, para. 53.
[29] P.D., Part V, para. 50.
[30] P.D., Part V, para. 50(3).
[31] P.D., Part V, para. 47(6).
[32] P.D., Part V, para. 50(5).
[33] P.D., Part V, para. 54.
[34] P.D., Part V, para. 51.

Questions:

1. What might some of the problems be in relation to electronic discovery and inspection, from the perspective of an information security professional?

b. Discovery in criminal proceedings

There is a much more limited power to inspect documentary evidence in criminal proceedings, although there have been recent changes made to the Criminal Procedure Code to introduce case disclosure requirements.[35]

[35] Criminal Procedure Code, Part IX.