DIGITAL EVIDENCE ASIA-PACIFIC: CERTIFICATION AND TECHNOLOGICAL NEUTRALITY*

Author Information

Name of Authors: Debayan Bhattacharya and Pulkit Goyal

Institution: National Law University Delhi

Year: 4th Year Students

Contact Information: debayan.bhattacharya20@nludelhi.ac.in; pulkit.goyal20@nludelhi.ac.in

* This article has been commissioned for LAWASIA by the Anil Divan Foundation

I: INTRODUCTION

Digital Evidence has been a matter of contention in evidence law for decades now. It is generally considered more volatile, and open to manipulation, and loss of data than other types of evidence due to its unique features.[1] This has resulted in several legal systems creating special provisions and procedures to govern the admissibility and authentication of digital evidence, distinct from the usual procedure.[2] However, this approach is not uniform. The United Nations Commission on International Trade Law Model Law on Electronic Transferable Records ['UNCITRAL Model Law'] emphasizes that digital evidence should be treated the same way as other kinds of evidence.[3] This is known as the principle of digital equivalence and has led some jurisdictions to eschew special provisions for digital evidence.

This sharp difference in the approach to digital evidence is reflected in jurisdictions across Asia-Pacific. This paper specifically looks at the approaches in India, Malaysia, Singapore, and Australia in order to survey the difference between their approaches to digital evidence. These jurisdictions are all common law countries and their legal systems have been heavily influenced by English law due to centuries of British colonial rule. Due to this common heritage, these countries have some striking similarities in their legal systems and merit comparison. At the same time, their approach to digital evidence has diverged in recent years.

---

[1] Albert Antwi-Boasiako and Hein Venter, 'A Model for Digital Evidence Admissibility Assessment' in Gilbert Peterson Sujeet Shenoi (eds) '13th IFIP International Conference on Digital Forensics' (IFIPAICT 2017) 25; Allison Rebecca, 'The Authentication of Electronic Evidence' (DPhil Thesis, Queensland University of Technology 2016) 60-95; Radina Stoykova, 'Digital evidence: unaddressed threats to fairness and the presumption of evidence' [2021] 42 Computer Law and Security Review 1; Interpol, *Guidelines for Digital Forensics First Responders* (Interpol 2021); Eoghan Casey, 'Error, Uncertainty, and Loss in Digital Evidence' [2002] 1(2) International Journal of Digital Evidence 1; R. Boddington, V.J. Hobbs and G. Mann, 'Validating digital evidence for legal argument' (6th Australian Digital Forensics Conference, Perth, 2008) <https://researchportal.murdoch.edu.au/esploro/outputs/conferencePaper/Validating-digital-evidence-for-legal-argument/991005541784607891> accessed 30 July 2023; Shahzad Saleem, 'Protecting the Integrity of Digital Evidence and Basic Human Rights During the Process of Digital Forensics' (DPhil Thesis, Stockholm University) 3, 23; Giancarlo Fiorella, Charlotte Godart, and Nick Waters, 'Digital Integrity: Exploring Digital Evidence Vulnerabilities and Mitigation Strategies for Open Source Researchers' [2021] 19(1) Journal of International Criminal Justice 147; Gunnar Alendal, Geir Olav Dyrkolbotn and Stefan Axelsson, 'DIGITAL FORENSIC ACQUISITION KILL CHAIN – ANALYSIS AND DEMONSTRATION' in Gilbert Peterson Sujeet Shenoi (eds) '13th IFIP International Conference on Digital Forensics' (IFIPAICT 2017).

[2] *Infra* Parts II and III.

[3] Model Law on International Commercial Arbitration 1985 (United Nations Commission on International Trade Law [UNCITRAL]) UN Doc A/40/17, Annex I, art. 5, 6.

Singapore[4] and Australia[5] have tried to achieve digital equivalence through 'technological neutrality'. In essence, their statutes make no difference between the provisions relating to the admissibility of digital evidence and other evidence.[6] These two countries have subscribed to the principle that laws should be 'technologically neutral' and not discriminate based on technology. In evidence law, this means that they have rejected special provisions to deal with evidence law.

On the other hand, India and Malaysia are 'technologically specific' and have special provisions for digital evidence within their statute.[7] Importantly, Singapore earlier had provisions similar to India and Malaysia, but these were abolished after the Evidence (Amendment) Act, 2012.[8] These four jurisdictions, therefore, cover a wide spectrum of approaches to digital evidence and comparisons amongst them can result in useful guidelines or best practices that can be adopted by other jurisdictions in the region and internationally.

This debate over how digital evidence should be treated differently (if at all) from other types of evidence has important consequences for lawmaking. This paper addresses the overarching debate through an analysis of the principle of 'technological neutrality', which is often offered as a justification for not having special provisions, and the certification system, a model of admission of digital evidence followed in Malaysia and India.[9] In Part II, the paper takes a closer look at arguments in favour of technological neutrality in evidence law and highlights its shortcomings. After establishing the necessity of special provisions, Part III addresses one of the most prominent methods to address these vulnerabilities: certification. The paper highlights the differences in certification requirements across Asia-Pacific, highlights their flaws, and provides recommendations for how certificates can be improved. Part IV concludes by summarising the main arguments raised and suggestions given. It also points out the limitations of the current study and the scope for future research.

---

[4] Evidence (Amendment) Act 2012.
[5] Uniform Evidence' in Jeremy Gans, Andrew Palmer, and Andrew Roberts (eds) Uniform Evidence (3rd ed, Oxford 2019).
[6] *Infra* Parts II and III.
[7] *Infra* Parts II and III.
[8] Wendy Low, 'A Commentary on the Amendments to the Electronic Evidence Provisions in the Singapore Evidence Act' (*Law Gazette*) <https://v1.lawgazette.com.sg/2012-07/468.htm> accessed 28 August 2023.
[9] See, for example, Technology Law Development Group, *Computer Output as Evidence: Consultation Paper* (Singapore Academy of Law 2003) 90-94, 151-154 ('TLDG Consultation Paper').

II: TECHNOLOGICAL NEUTRALITY OF EVIDENCE LAW

A: THE COMPETING MEANINGS OF TECHNOLOGICAL NEUTRALITY

Technological neutrality[10] is best understood by contrasting it with technological specificity. For example, a law meant to regulate the use of photos from reel cameras (technologically specific) versus a law meant to regulate all forms of media that capture and visually present past events (technologically neutral).[11] The latter defines the object of regulation functionally (capture and visually present) rather than the specific process (reel cameras) that the object uses.

Technological neutrality is identified as having two goals: (1) to promote stability by ensuring the longevity of statutes and (2) to ensure doctrinal equivalence.[12] Technology neutrality future-proof laws.[13] A technologically specific provision (as in the case of a law relating to film cameras) cannot be interpreted in a way to include new technologies while maintaining fidelity to the text. A technologically neutral provision on the other hand would (ideally) require no amendments to incorporate new technologies within it by using functional definitions instead of process-dependent ones.[14] Technological neutrality can be understood as formal or substantive technological neutrality. Formal technological neutrality applies the same legal provisions to different technologies. This is achieved by employing vague language for definitions which are broad enough to incorporate future technologies into it.[15] In the context of evidence law, this means having the same legal provisions for the admissibility of all kinds of evidence (whether digital or otherwise).[16] Substantive technological neutrality, on the other hand, permits special provisions are permitted as long as new technologies are functionally treated equally by the law.

In *Rethinking Technological Neutrality,* Brad Greenberg critiques the fundamental rationale for formal technological neutrality.[17] Even though he writes in the context of copyright law, Greenberg points out several general concerns with laws that purport to be technologically neutral.

---

[10] Brad A Greenberg, 'Rethinking Technology Neutrality' (2016) 100 Minnesota Law Review 1495.
[11] ibid.
[12] ibid.
[13] ibid.
[14] ibid.
[15] ibid.
[16] TLDG Consultation Paper (n 9).
[17] Greenberg (n 10).

He questions how laws can be neutral and apply in a non-discriminatory way in light of unforeseen future technologies.[18] Technologically neutral laws try to focus on the what instead of the how. However, in the case of digital evidence, as the paper argues below, the process is interlinked with the object. Digital evidence invariably requires using software which processes data and presents it in a human-readable format. So, the ultimate evidence that is used in court cannot be separated from the process (software) that is used to make it human-readable.

Greenberg points out four shortcomings of formal technological neutrality. First, laws are often drafted to address present problems posed by current technologies and are then expanded to cover still-unknown technology.[19] It is difficult for legislators or policymakers to accurately predict what new technology will hit the market, what disruption it will cause, and what unique vulnerabilities it will expose in the existing law.[20] This approach assumes linear progressions in technology and does not account for disruptive changes.

Second, as elucidated by HLA Hart,[21] all provisions of the law have a core of certainty where the words of the statute clearly cover a given situation and a penumbra of uncertainty where the words can be interpreted either way.[22] While all statutes suffer from this problem, technologically neutral statutes are especially vulnerable because they intentionally employ vague terminology in order to cover new unknown technology within their ambit.

Third, technological neutrality also leads to infrequent revisions of the law as it creates an illusion that the provisions are adequate for the new technology it is being applied to. Despite statutes claiming to apply to all current and future technologies, countervailing concerns render their application uncertain and undesirable to future technologies.[23] This blurs the application of technologically neutral laws to new technologies along instrumental (exempting new technologies to better serve the purpose of the law) and formalistic (applying the text regardless of the purpose or countervailing concerns) lines.[24]

---

[18] ibid 1523.
[19] ibid.
[20] ibid 1526.
[21] ibid 1530; HLA Hart, *The Concept of Law* (2nd edn, OUP 1994) 123.
[22] Greenberg (n 10) 1529.
[23] ibid 1531-1533.
[24] ibid 1537.

Lastly, and as a result of the above, technologically neutral laws are often not neutral in their application. Neutrality is only a pretence. The divergence between formal and instrumental interpretations brings forth the bias inherent in the interpretation of technologically neutral provisions. It is a choice the decision-maker makes.[25] So, applying a technologically neutral law, designed to address vulnerabilities in existing technologies, to new technologies with new vulnerabilities subjects the new technology to a less rigorous standard. Further, the blanket application of a neutral provision may in effect discriminate against technologies due to the existence of special characteristics. This defeats the goal of doctrinal equivalence.[26]

Technological neutrality should instead be viewed as a sliding scale where drafters make the choice of tailoring the law to balance technological specificity and formal technological neutrality. This results in statutes that are substantively technologically neutral and better serve the aims of technological neutrality than formally technologically neutral statutes. The quantification of when the balance has been sufficiently drawn is always unclear, especially given the fact that accurately predicting future technologies is nearly impossible.

It is important to keep in mind the delicate balance that has to be drawn between specificity and neutrality when designing laws, and this also applies to evidence law. The goal of evidence law is to ensure that evidence that is received in court meets certain criteria. It should be authentic, reliable, and not militate against other policy requirements.[27] As the paper demonstrates below, achieving some of these goals in the unique context of digital evidence *requires* special provisions and differential treatment. The paper argues that special provisions are needed to make evidence law future-proof and that the law better satisfies the spirit of technological neutrality when such provisions exist.

B: THE TWO MODELS FOR DIGITAL EVIDENCE

In the previous section, the paper discussed the principle of technological neutrality. This section analyses the broader debate surrounding the application of technological neutrality in evidence law by referring to the position of law in various Asian-Pacific countries. Specifically, the paper

[25] ibid 1544.
[26] ibid 1544.
[27] Hock Lai Ho, 'Evidence and Truth' in Christian Dahlman, Alex Stein, and Giovanni Tuzet, Philosophical Foundations of Evidence Law (OUP 2021) 21.

explores the law in Singapore and Australia and analyses the debates around special provisions that have occurred in these nations. The paper then argues that the formally technologically neutral approach to digital evidence is counterproductive and undermines the goals of evidence law.

i: SINGAPORE

Singapore is an interesting jurisdiction to begin with since it previously had special provisions for digital evidence similar to India and Malaysia, which were removed by the Evidence (Amendment) Act, 2012. Section 35 of the Evidence Act, 1893 ['Singapore Evidence Act'] before amendment stated that computer output will be 'admissible' if it is expressly agreed upon, produced 'in an approved process', or is shown by party tendering such output. The Singapore Evidence Act also permitted an individual in a 'responsible position' to tender a certificate that the computer was working in accordance with an 'approved process', after which the Court would presume that the output was true unless proven otherwise.[28]

Moreover, if an individual signed a certificate describing the output and how it was produced, then it would be presumed true.[29] If the individual responsible did not have control or access to the computer, a certificate from whoever had control or access to the computer would suffice.[30] All of these only had to be proved to the 'best of the knowledge and belief of the person stating it.'[31] In case the Court believes it is needed, they could also call for oral evidence to prove the computer output.[32]

The pre-amendment Singapore Evidence Act treated electronic evidence as a separate class of evidence. Though the provision may seem narrowly tailored to a computer (and thus implicitly excluding other forms of digital evidence), a 'computer' was broadly defined to mean '*electronic, magnetic, optical, electrochemical, or other data processing device…performing logical, arithmetic or storage functions, and includes any data storage facility or communications facility*.'[33] Therefore, any evidence that could reasonably be classified as digital evidence was still covered by Singapore's laws. Notably, this broad definition of computer is also seen in

[28] Singapore Evidence Act 1893, s 35(3) (before the amendment).
[29] ibid s 35(6).
[30] ibid s 35(7).
[31] ibid s 35(9).
[32] ibid s 36(3).
[33] ibid s 3.

jurisdictions such as Malaysia,[34] which has laws similar to the erstwhile Sections 35 and 36 of the Singaporean Evidence Act and has been held to include diverse forms of electronic evidence.

Despite the seemingly comprehensive nature of these provisions, they were nonetheless criticised for lacking 'technological neutrality.' The Singapore Academy of Law's Technology Law Development Group ('TLDG') released a Consultation Paper ('TLDG Consultation Paper') in 2003 that was critical of the special provisions relating to digital evidence.[35] It argued that the 'principle of equivalence' as contained in the UNCITRAL Model Law on Electronic Commerce was missing in Singapore law.[36] The principle of equivalence states that electronic evidence should not be rendered inadmissible *solely* because it is in a different form than other kinds of evidence.[37]

The TLDG Consultation Paper then analysed whether Sections 35 and 36 of the Singapore Evidence Act (pre-amendment) are consistent with the principle of equivalence.[38] It invoked technological neutrality and argued that there was no need for special provisions at all.[39] It argued that existing principles of evidence law, including identification, chain of custody, integrity, etc. are by themselves sufficient to authenticate digital evidence and negate the need for any special provisions.[40] This line of argumentation ignores the nuance that the paper pointed out previously; that technological neutrality is better viewed as existing on a sliding scale and not as a binary. Rather than contending with what level of specificity is helpful, the TLDG Consultation Paper makes a critique of the law as it stands and then argues that applying the standard provisions of evidence law to digital evidence is sufficient.

Nevertheless, with this analysis, the TLDG Consultation Paper advocated for the repeal of Sections 35 and 36. This paper was followed up in 2004 by a Final Report, where the TLDG reiterated its conclusions.[41] These two papers led to the amendments to the Singapore Evidence Act.[42]

---

[34] Malaysia Evidence Act 1950, s 3.
[35] TLDG Consultation Paper (n 9).
[36] ibid 67-8.
[37] ibid 69.
[38] ibid 70.
[39] ibid 82-5.
[40] ibid 106-11.
[41] Technology Law Development Group, *Computer Output as Evidence: Final Report'* (Singapore Academy of Law 2004).
[42] Ministry of Law, 'Consultation on Amendments to the Evidence Act' available at <https://www.mlaw.gov.sg/files/linkclickbd8a.pdf> accessed 30 July 2023.

The TLDG Consultation Paper is open to criticism. Even though it acknowledged that digital evidence is different from other kinds of evidence - even outside of just form,[43] unfortunately, it failed to expound on these differences and their consequences. As the paper will demonstrate later, the differences between these two types of evidence provide compelling grounds to have different provisions for each of them even if the equivalence principle is accepted.

A result of the TLDG Consultation Paper's failure to expound on the consequences of these differences is its failure to explain Section 116A of the Singapore Evidence Act. Section 116A was introduced by the Evidence (Amendment) Act, 2012 and it states that any computer that ordinarily 'produces' or 'communicates' any 'electronic record' will presume that the record was accurately produced.[44] This provision is *only* applicable to electronic records, thereby making it a special provision.

Outside of these changes, however, electronic evidence in Singapore is now subject to the usual rules of admissibility that apply to other types of evidence. There is still a presumption that any electronic evidence is accurate if it was produced or communicated in the ordinary course of action, which is strikingly similar to provisions in jurisdictions like India which were not considered technologically neutral by the TLDG itself.[45] This implies that Singapore itself is not truly (formally) technologically neutral, since it does continue to discriminate between electronic evidence and other types of evidence.

ii: AUSTRALIA

Australia consists of several federal states with their own Laws of Evidence. However, since 1995 there has been a move towards a Uniform Australian Legislation on Evidence.[46] The Uniform Legislations are based on the Commonwealth Evidence Act, 1995, and have been adopted by five other jurisdictions in Australia. While this part will make references to non-uniform law jurisdictions as well, the comparative focus is going to be on the Uniform Evidence Law.

---

[43] ibid.
[44] Singapore Evidence Act, s 116A.
[45] TLDG Consultation Paper (n 9) 64-68.
[46] Australian Law Reform Commission, 'Uniform Evidence Law' (*ALRC,* 6 February 2006) <https://www.alrc.gov.au/inquiry/uniform-evidence-law/> accessed 28 August 2023.

The Uniform Australian Legislations currently do not have any special requirements for the admission of digital evidence. Sections 146 and 147 of the Uniform Legislations provide presumptions in favour of evidence produced by 'devices or processes' which are ordinarily considered reliable, or in the course of business.[47] There are some special provisions presuming the reliability of electronic communication.[48] For the purposes of admissibility, digital evidence is generally considered to be a document.

In 2005, the Australian Law Reform Commission ('ALRC') considered whether the Uniform Legislations needed reforms.[49] It considered whether a more rigorous approach to admitting digital evidence was required based on the responses and submissions it received. In doing so, it considered the merits of a certification system, as was followed in South Australia, and noted that certification has the advantage that it 'recognises in a direct way the need to address the issue of whether a computer has operated correctly in producing material that is to be admitted.'[50]

However, the ALRC was swayed by the apparent demerits of a more rigorous approach.[51] The demerits identified in submissions received by the ALRC revolved around increased compliance costs and time without any real benefit, as was evidenced by the lack of cases of wrongful convictions based on computer-generated evidence.[52] This was emboldened by the increasing frequency of the use of such evidence.[53] Adversarial procedure was also posited as taking care of any concerns that might exist about the reliability of digital evidence.[54]

The arguments against a more rigorous standard are principally efficiency-based arguments and not justice-based arguments. In India and Malaysia, where a more rigorous model is followed, there have not yet been many complaints about admissibility conditions being onerous.[55] In

---

[47] Commonwealth Evidence Act 1995, ss 146, 147.
[48] Commonwealth Evidence Act 1995, ss 71, 161.
[49] Australian Law Reform Commission, *Uniform Evidence Law: Report* (Law Com Rep 102, 2005).
[50] Australian Law Reform Commission (n 49).
[51] Australian Law Reform Commission (n 49) [6.41].
[52] ibid [6.31]-[6.36].
[53] ibid [6.34].
[54] ibid [6.35].
[55] The majority of the literature discusses whether certificates in these jurisdictions are mandatory or not. In India, the criticism of mandatory certification is not on the basis that these are onerous to produce, but that it is an incorrect interpretation of the statute and precedent. For instance, see Bhavyakirti Singh and Aditya Bamb, 'The Dichotomy of the 65B Certificate: Analysing Trends with Regard to the Authentication of Electronic Evidence in India' [2021] 10(1) Christ University Law Journal 73.

Singapore, such arguments were raised in the context of the 'approved process' standard which required regular re-certification by the government authority and was economically unviable for small to medium businesses.[56] A lot of costs relating to digital evidence go into storing and retrieving information from large quantities of information.[57] Issues such as lack of backward compatibility also add to the cost.[58] These have nothing to do with additional admissibility conditions and will be incurred regardless. While a certification standard would make the process more onerous than it is currently, there is no reason to conclude that the costs would be disproportionate or overly onerous.

As far as the perceived benefit is concerned, evidence law plays several roles. One of these is preserving the integrity of the legal process in the eyes of the public.[59] As the Victorian Privacy Commissioner correctly observed:

> [I]n numerous instances in Victoria, technology-generated evidence (particularly speed camera evidence) has been shown to be less than reliable. … it is critical to maintain public confidence in the judicial process and that this can be eroded by even isolated instances of the admission of inaccurate computer evidence…. the public's confidence in the accuracy and reliability of some technologies has already been shaken.[60]

There are other instances as well. In India, there have been instances of manipulated digital evidence in criminal cases. Notably, in the *Elgar Parishad* case, the objectionable material found on the accused's laptop was found to be externally planted by an independent forensics report.[61] More recently there have been global concerns about the use of deepfakes as evidence.[62]

---

[56] TLDG Consultation Paper (n 9).
[57] B Schafer and S Mason, 'The Characteristics of Electronic Evidence' in Stephen Mason and Daniel Seng (eds), *Electronic Evidence* (University of London Press 2017) [2.43].
[58] ibid [2.41].
[59] C Nesson, 'The Evidence or the Event? On Judicial Proof and the Acceptability of Verdicts' (1985) 98 HLR 1357.
[60] Australian Law Reform Commission (n 49) [6.37].
[61] Arsenal Consulting, 'IN THE COURT OF SPECIAL JUDGE NIA, MUMBAI SPECIAL CASE NO. 414/2020 National Investigating Agency VS Sudhir Pralhad Dhawale & others Report IV' (18 August 2021) available at <https://www.medianama.com/wp-content/uploads/2021/12/BK-Case-Rona-Wilson-Report-IV-Digitally-Signed-and-Locked.pdf>.
[62] Shannon Bond, 'People are trying to claim real videos are deepfakes, the court is not amused' (*NPR,* 8 May 2023) available at <https://www.npr.org/2023/05/08/1174132413/people-are-trying-to-claim-real-videos-are-deepfakes-the-courts-are-not-amused>.

The increasing frequency of use of digital evidence supports additional admissibility requirements more strongly than it opposes them. As the use of digital evidence increases, and the threat of manipulation remains unaddressed, not only does this risk wrong outcomes from the courts, this risks a loss of confidence in the public about the sanctity of court procedure. Even an analysis of case law in Australia points out that sufficient safeguards for electronic evidence are lacking. As AR Stanfield shows, in *ASIC v Rich,*[63] the NSW Supreme Court did not consider the integrity of electronic records when deciding the authenticity of digital evidence.[64] All these questions instead were relegated to the stage of probative value.[65] This was despite metadata existing about modification of this evidence at key dates. Furthermore, there was no evidence about the software used and how the reports were generated. As Stanfield notes:

> Evidence about the system, its integrity, and how reports were generated should have been, with respect, tendered and the witnesses should have, again with respect, given evidence as to the systems operation and reasonable level of security. With respect, an argument about provenance cannot be correctly posed and answered without such evidence.'[66]

C: FURTHER LIMITATIONS OF A FORMAL TECHNOLOGICAL NEUTRALITY APPROACH TO EVIDENCE LAW

The TLDG Papers and the ALRC Report provide an endorsement of the principle of formal technological neutrality and not discriminating between electronic evidence and other types of evidence. However, both of them admit that there is a distinction between both these kinds of evidence. There is no elaboration of the consequences of this admission. This is important: if there is a difference between digital evidence and other evidence, then it is reasonable to have distinct provisions to deal with them.

The UNCITRAL Model Law on Electronic Commerce ('UMLEC'), mentioned in the TLDG Consultation Paper, makes it clear that the equivalence principle that these Reports rely on does

---

[63] (2009) 236 FLR 1.
[64] (2005) 216 ALR 320.
[65] AR Stanfield, 'The Authentication of Electronic Evidence' (Doctor of Philosophy Thesis, Queensland University of Technology 2016) [6.6.1.8].
[66] ibid.

not oppose special provisions. Article 10 of the UNCITRAL Model Law on Electronic Transferable Records, which is an updated version of the UMLEC, discusses the degree of strictness a law should have when dealing with a transferable record.[67] It states that the law should only require a reliable method to verify the record and nothing more.[68] Therefore, it seems to be implicit that the purpose of the principle is to ensure that no onerous restrictions on electronic evidence solely because of the fact that it is electronic evidence: discrimination is permitted where it serves a genuine purpose.

This affects the usefulness of formal technological neutrality as a guiding tool for statutory provisions. Supporters have relied on the principle to make indefensibly broad claims and argue against any and all special provisions for digital evidence. In Singapore, the TLDG pointed out valid criticisms of Sections 35 and 36 but then advocated for complete formal technological neutrality by banking on the equivalence principle. Complete neutrality is opposed to the principle of equivalence. This harkens back to the original argument about technological neutrality that its spirit, and by extension the principle of equivalence, is better served through special safeguards for certain kinds of evidence.

The following subsections provide further criticism of formal technological neutrality in evidence law and argue for special provisions in cases of digital evidence. The first subsection argues that different kinds of evidence are treated differently anyway and this should also be the case for digital evidence. The second subsection argues that there are vast differences between different technologies themselves, which means that they require different treatment. The last subsections argues that using technological neutrality undermines the ability to relax the best evidence rule - this paradoxically makes the admissibility of evidence more difficult.

i: EVIDENCE LAW TREATS DIFFERENT KINDS OF EVIDENCE DIFFERENTLY

There is nothing internal or inherent to the logic of evidence law that prevents it from treating different forms of evidence differently. There are certainly content-based classifications in evidence law, such as the rule against opinion evidence and the exception to that in terms of the

[67]UNCITRAL Model Law on Electronic Transferable Records 2017 ((United Nations Commission on International Trade Law [UNCITRAL]) A/RES/72/114, art 10.
[68] ibid.

rule permitting expert evidence.[69] There are also classifications and exceptions which are neither based on form nor content, but on the circumstances surrounding the evidence such as the rule against hearsay.[70] More importantly for the purposes of this paper, the common law has classically categorised evidence based on its form into oral evidence, documentary evidence, and material evidence and has developed specific rules with respect to them.[71] These address the special character of the form in which evidence is being given.

Evidence law does discriminate between different forms of evidence because of the distinct characteristics of the different forms. However, it is worth mentioning that these categories themselves have been wide enough to cover different forms of evidence within themselves that do not have sufficiently distinct characteristics. For example, oral evidence also covers testimony given via the use of sign language or other gestures, documentary evidence also has been broad enough to accommodate drawings, photos, etc. The next part argues that electronic evidence has characteristics sufficiently distinct from documentary evidence and thus merits different treatment.

ii: JUSTIFYING DIFFERENTIATING DIGITAL EVIDENCE FROM OTHER KINDS OF EVIDENCE

India, Malaysia, Singapore, and Australia have, under their respective Acts, sought to treat electronic evidence as documentary evidence.[72] This part will discuss various distinguishing characteristics of digital evidence from documentary evidence as justification for treating digital evidence as a separate category.

First, digital evidence is more vulnerable to manipulation, alteration, and fabrication than documentary evidence.[73] Changes to digital evidence can be made without leaving physical marks in the final output.[74] Audio and video files can be edited as well using software in seamless ways.

---

[69] Indian Evidence Act 1872, s 45-51; Malaysian Evidence Act 1950, s 45-51; Singapore Evidence Act 1893, s 47-53; Commonwealth Evidence Act 1995, part 3.3.
[70] Indian Evidence Act 1872, s 60; Malaysian Evidence Act 1950, s 60; Singapore Evidence Act 1893, s 62; Commonwealth Evidence Act 1995, part 3.2.
[71] Indian Evidence Act 1872, s 3; Malaysian Evidence Act 1950, s 3; Singapore Evidence Act 1893, s 3; Commonwealth Evidence Act 1995, ch 2.
[72] Indian Evidence Act 1872, s 3; Malaysia Evidence Act 1950, ss 3, 90A; Singapore Evidence Act 1893, ss 3, 64; Commonwealth Evidence Act 1995, ss 146, 147; Australian Law Reform Commission (n 50) [6.15]-[6.16].
[73] See (n 1).
[74] Shafer and Mason (n 57) [2.9].

Even log files which are generated automatically by computers to keep track of activity over a server are not immune from tampering.[75] As time passes and technology develops, so does the scope for tampering. Artificial Intelligence can now be used to edit video evidence using deep fakes.[76] This can have serious ramifications on the usage of CCTV footage in trials.

Vulnerabilities of digital evidence can also be used to plant digital evidence as seems to have been done for Wilson, an accused in the Bhima Koregaon case.[77] The police alleged to have found objectionable material on the accused's laptop, however, an independent forensic investigation of the laptop revealed that the files were not created by the accused and were never opened by him either.[78] The version of the MS Word used was also different from that used by the accused.[79] Because of these additional vulnerabilities, there is a need for additional safeguards when receiving digital evidence. Similar manoeuvres would be impossible or at least more difficult to pull off with traditional documentary evidence.

Second, it is almost impossible to access and differentiate 'original evidence' or 'primary evidence' in the case of electronic records. Data in a computer exists as 1s and 0s and requires an interpreter in the form of software (such as MS Word, Apple Pages, etc.) which translates that into human-readable format. Digital evidence is thus inseparable from the process that creates it. Even different versions of the same software that are not backwards compatible will affect the formatting of the document and even the ability to access it.[80] This also gets increasingly complicated when one considers that multiple versions of the same file exist in a device.[81]

Further, it is also undesirable in most cases that the most direct evidence of electronic record is produced. First, if the record is in a device that a person routinely uses and requires frequently for work or personal reasons, it will be undesirable to ask them to deposit this device with the court for the purposes of trial. It is also possible, and certainly happens in the case of corporations, that

[75] Casey E, 'Error, Uncertainty, and Loss in Digital Evidence' (2002) International Journal of Digital Evidence 1.
[76] Arsenal Consulting (n 61).
[77] ibid.
[78] ibid.
[79] ibid.
[80] Shafer and Mason (n 57) [2.14].
[81] Shafer and Mason (n 57) [2.9].

the original data is in bulky servers that cannot be produced in court.[82] Additionally, if the file is on an online cloud server, it might not be possible to requisition that the server where the original file is stored be produced before the court since it might be in another country altogether. Secondly, there is a viable alternative since computers can create virtually identical copies of records.

Third, digital evidence often involves processing by computers which documentary evidence does not. A forensic scientist creating a DNA report might put her findings and measurements into a computer and the computer will process these to arrive at conclusions. Similarly, an intoximeter/breathalyser will analyse the breath and produce a result indicating the level of intoxication of a person. These processes may or may not be reliable and will require further evidence about the processes that produce them to check their veritableness in a manner similar to how the law relating to expert evidence requires experts to give information about the processes involved in their analysis. Similar considerations do not arise when dealing with documentary evidence.

iii: TECHNOLOGICAL NEUTRALITY CAN MAKE DIGITAL EVIDENCE MORE DIFFICULT TO ADMIT

The 'Best Evidence Rule' is one of the cardinal principles of evidence law. Under this principle, an original is considered sufficient proof of its contents while copies are considered less reliable. The rule requires that the original document be produced to prove that document's contents since the original document is considered the best evidence for its contents.[83] It is prominently reflected in several statutes around the world, which all require the production of an original document, at least when proving the contents of a document.[84]

---

[82] This is exactly what happened in *Zubulake vs. UBS Warbrug LLC,* 217 FRD. 309. The plaintiff, Laura Zubulake, sought access to UBS' archived emails to prove her claim of gender discrimination. UBS refused to furnish them because they would cost $ 175,000 excluding attorney costs. The Court eventually held that UBS had to furnish the data but looked at the accessibility of the data to determine whether it was 'unduly burdensome or expensive' to produce the data.

[83] Dale A Nance, 'The Best Evidence Principle' [1988] 73 Iowa Law Review 227; California Law Reform Commission, *Best Evidence Rule* (California Law Reform Commission 1996) 371.

[84] Cynthia Ford, 'What the Best Evidence Rule is - and what it isn't' [2014] EvidenceCorner 22, 22; Dale A Nance, 'The Best Evidence Principle' [1988] 73 Iowa Law Review 227; Colin Miller, *Evidence: Best Evidence Rule* (CALI eLangdell Press 2012); Eilis Magner, 'The Best Evidence Rule - Oral Testimony or Documentary Proof?' [1995] 18(1) UNSW Law Journal 67, 69.

While the distinction between the original and the copy is intuitive in the context of physical documents, it breaks down in the case of digital communications and electronic records. This results in a scenario where the application of the Best Evidence Rule ends up having absurd consequences. In order to correct these incongruous consequences, special provisions to relax the Best Evidence rule while dealing with electronic evidence are required. In fact, all the jurisdictions examined have devised some way to skirt the best evidence rule for digital evidence. Singapore contains a presumption of authenticity given certain conditions are met.[85] Australia completely got rid of this rule with the enactment of the Uniform Evidence Act 1995.[86] In India[87] and Malaysia[88], the certificate provisions explicitly make secondary forms of digital evidence admissible. On the other hand, formal technological neutrality would require including digital evidence under the definition of a 'document', which would make the Best Evidence rule apply in full force. This means that digital evidence is exposed to an unrealistically exacting standard. Paradoxically, this makes the admission of digital evidence more difficult and uncertain - contrary to what proponents of technological neutrality seek.

To illustrate this, let us highlight the issues that occur in applying the original/copy distinction in the digital realm.[89] Firstly, the ability to copy a document at will muddles the distinction significantly. Consider the fact that there may be two exact copies of a document on the same device. Which is the original? It may seem like the file that was created first would be the original, but this need not be the case. The original file may have been modified, or otherwise, the newer copy may be used by parties as the original and considered the original in all their transactions. Which, then, is the original?

This abstract example demonstrates the issues with operating this distinction in the case of digital evidence. This can lead to circumstances where there is a lack of clarity as to what is the original due to conflicting judicial opinions. Moreover, the distinction is undesirable since the original file is as vulnerable to tampering as the copy because, as argued above, tampering with digital evidence can be done in seamless ways without making the alterations evident. This calls the Indian practice

---

[85] Singapore Evidence Act 1893, s 116A.
[86] Commonwealth Evidence Act 1995, s 51.
[87] Indian Evidence Act 1872, s 65B.
[88] Malaysian Evidence Act 1950, s 90A.
[89] Stephen Mason and Daniel Seng, *Electronic Evidence* (4th edition, Institute for Advanced Legal Studies 2017) 53-55.

of requiring certification for copies and not requiring them for originals into serious question. Issues such as this result in the adoption of special provisions regardless, as this paper highlighted in the case of Singapore. The debate over whether formal technological neutrality is desirable or not is thus not very helpful; the debate then has to be about *which* special provisions are justified. The paper explores this question in Part III.

III: CERTIFICATION STANDARDS

As the paper established in Part II, there are good reasons to treat digital evidence differently from other types of evidence and to reject a formally technologically neutral approach to evidence law. What then should these special conditions look like? In India and Malaysia, and erstwhile in Singapore and South Australia, the answer was some form of certification regime. A certification regime essentially requires a certificate describing the process of the production of the record from an individual who was 'responsible' for the computer system. Once a valid certificate is provided, courts consider it sufficient evidence of the content within the certificate.

Certification has been widely used across Asia-Pacific: India, Malaysia, Singapore before 2012, and South Australia before 2015. However, there are differences in the legal status and requirements of these certificates in these jurisdictions such as the mandatory nature of these certificates. Moreover, there are several flaws in what certificates need to contain. Often, they do not require important information like metadata, making them functionally unhelpful in protecting the integrity of digital evidence.

This part explores these issues by first discussing the legal regime for certificates in India and Malaysia. It then proceeds to discuss the flaws in existing certification regimes and provides suggestions for how they can be improved.

A: DIFFERENCES ACROSS NATIONAL LEGISLATIONS

Certifications are mentioned in the statute in India and Malaysia. In India, Section 65B(4) of the Indian Evidence Act, 1872 requires that a person occupying a 'responsible official position *in* relation to the operation of the relevant device or the management of the relevant activities' provide a certificate 'identifying the electronic record…and describing the manner in which it was

produced.'[90] They may also be asked to provide particulars to show that the record was produced by a computer.[91] Similarly, Section 90A of the Malaysian Evidence Act, 1950 states that one can prove that a record was produced by a computer 'in the course of its ordinary use' by tendering a certificate from an individual who was 'responsible for the management of the operation of that computer.' These provisions are similar insofar as they require a certificate from an individual in a responsible position. Moreover, certificates are generally considered reliable proof of their content.

However, despite these similarities, there have also been differences. One of the largest debates in the case of certificates is whether they should be mandatory for admitting digital evidence, or if an oral statement as to the digital record is sufficient. India and Malaysia have completely diverging views on the issue. In the case of *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* ['Arjun Panditrao'], the Indian Supreme Court finally settled the jurisprudence on the matter and ruled that a certificate under Section 65B was mandatory for the admission of digital evidence.[92] Even if there was clear oral evidence about the contents of the evidence by the responsible person, the evidence would not be admitted absent an appropriate certificate.[93] However, the Supreme Court does differentiate between primary and secondary electronic evidence and holds that only secondary electronic evidence requires a certificate.[94]

In Malaysia, oral evidence can be used to prove the content of a piece of digital evidence and certificates are not mandatory.[95] In the landmark case of *Gnanasegaran Pararajasingam v Public Prosecutor*,[96] the Court of Appeal discussed the issue of certificates in detail. The defendant was convicted of criminal breach of trust by the lower court.[97] The defendant argued that the bank documents could only be admitted if it was accompanied by a certificate.[98] The Court rejected this argument and held that a certificate was only one of the ways to prove that the computer had

---

[90] Indian Evidence Act 1872, 65B(4)(a), (c).
[91] Indian Evidence Act 1872, 65B(4)(b).
[92] (2020) 7 SCC 1.
[93] ibid [72].
[94] ibid [31].
[95] Mohamed Duryana, 'Computer Evidence: Issues and Challenges in the Present and in the Future' [2011] Legal Network Series 1, 8-12.
<http://irep.iium.edu.my/8321/1/computer_evidence_by_Dr_Duryana_Mohamed_2011.pdf> accessed 30 July 2023.
[96] [1997] 3 MLJ 1.
[97] ibid 6.
[98] ibid 10.

produced the document in its ordinary course of operation.[99] It held that oral testimony as to the contents of the document by the person responsible for the system would also constitute sufficient proof for the digital evidence in question.[100] Further, Malaysia does not discriminate between primary and secondary electronic evidence.

India's position on the issue of mandatory certificates seems rigid and can cause difficulties, as it did in *Arjun Panditrao*. On the other hand, the Malaysian position provides a more flexible framework that also preserves the sanctity of digital evidence. Oral testimony from the individual responsible for the operation of the computer system fulfils the same purpose as a certificate. After all, a certificate contains the responsible individual's description of the formation of the record. The exact same information can also be passed on via oral cross-examination. The opportunity to question the testimony and cross-examination are effective ways to also ensure the veracity of the information. Further, for reasons argued above, it may be useful to reconsider the differences between primary and secondary digital evidence as used in Indian Evidence Law.

There are also issues in the law common to both jurisdictions. For instance, certificates in both Malaysia and India require them to mention that the electronic record was produced in the course of its regular or ordinary use.[101] Such a requirement seems an extension of the common law exception to hearsay evidence in the form of business records.[102] Records routinely maintained for the purpose of business were assumed to be filled with a high degree of accuracy and therefore despite being hearsay were considered to be admissible.[103] Such regular use is not necessarily true for all devices that may be used in the creation or production of digital evidence. Also, as the Law Commission of England and Wales noted, these bear only a questionable nexus to the reliability of the process of producing digital evidence.[104] Further, in their research, the authors have not come across any Indian or Malaysian case where the regularity was seriously disputed. This provision should accordingly be removed so that more kinds of digital evidence become

[99] ibid 11.
[100] ibid.
[101] Indian Evidence Act 1872, s 65B(2); Malaysian Evidence Act 1950, s 90A(2).
[102] This is called the 'business records exception' and it is an established exception to the hearsay rule in common law. *See* Federal Rules of Evidence, Rule 803(6).
[103] ibid.
[104] England and Wales Law Commission, *The Hearsay Rule in Civil Proceedings* (Law Com No 216, 1993) [3.15].

admissible. Hearsay and the business record exception can continue to apply but regularity should not be a requirement for admission of digital evidence.

A possible criticism against certification requirements is that once the certificate is produced, it would be incumbent upon the courts to admit digital evidence, despite palpable errors. To overcome this, certificates can be made the starting point for admissibility instead of its be-all and end-all.[105] So where some doubt is cast on the electronic evidence or the affidavit, then the person presenting the digital evidence should have the onus of presenting additional evidence to support their digital evidence.[106] The adverse party should also have a right to cross-examine the deponent of such certificates. This is currently not a requirement in India and Malaysia.

Further, a certification requirement also acts as a guide for the court and the opposing party on what questions to ask and factors to consider when taking oral evidence to authenticate digital evidence. Accordingly, a caveat to this claim is that the ability of certificates to authenticate digital evidence is dependent on the type of information required within a certificate. As the paper will demonstrate, the technical requirements of certificates leave a lot to be desired. The paper now proceeds to analyse the information required in certificates across South Asia and provide recommendations for improvement.

B: CERTIFICATION REQUIREMENTS ARE FLAWED

The kind of information required to be filled in a certificate is information regarding the process through which the output was produced and details of systems used to produce them. Further, the certificate is to be issued by a person responsible for the functioning of the system. There are two main issues with this model. First, these provisions presume a closed centralised system. Second, there are no metadata requirements about the digital evidence being produced, especially those that will affect the integrity of the electronic record.

i: CLOSED CENTRALISED SYSTEM

[105] This is similar to the Canadian position in dealing with electronic evidence. See Canadian Uniform Electronic Evidence Act 1997, s 7.
[106] Aradhya Sethia, 'Rethinking admissibility of electronic evidence' [2016] IJLT 1, 17-18.

Presently, statutes that need certificates only require that the certificate be furnished by the person 'responsible' for the system to the 'best of their knowledge.' These generally tend to be uncritically accepted by courts as valid proof of the information asserted. The problem with this is that it presumes that there is an identifiable person who is responsible for the functioning of a system and can testify to the proper functioning of the device. This is not true in the context of the rise of network systems, where systems are connected by networks like the Internet and LANs. On these, a computer system can be accessed remotely by any other system part of the same network and activity can be performed on the connected system. It may be difficult to discern the individual solely 'responsible' for these networks. Similarly, devices are often shared in South Asian households and a formal certificate by the owner of the device may have limited utility.[107]

This can be addressed by mandating additional 'assurances' be provided by people who had access to the device in the relevant time period. This helps move the certification requirement from the subjective best knowledge of a person in a responsible position to the device to the best available knowledge about the record. However, this has the potential to lead to issues in cases of big organisations which operate on servers such that potentially thousands of people would have access to a device and it would be unfeasible to get assurances from all of them. Accordingly, it is not recommended that all possible persons with access to the servers be questioned nor is it desirable to prescribe a minimum number of assurances required. Such questions are best solved in an ad-hoc manner by adjudication. This part simply provides a line of questioning that certification requirements should follow to improve the quality of digital evidence.

Further, certificates should contain information about the networks to which the device was connected. This should provide the information necessary to inquire into possible tampering and to challenge the integrity of the digital evidence produced. This will provide an opportunity to check whether the network was compromised at any material time. It will also aid the production of quality and verifiable digital evidence.[108]

---

[107] Nithya Sambasivan et al, ''Privacy Is Not for Me, It's for Those Rich Women': Performative Privacy Practices on Mobile Phones by Women in South Asia' (Fourteenth Symposium on Usable Privacy and Security,August 12–14 2018, Baltimore) <https://www.usenix.org/system/files/conference/soups2018/soups2018-sambasivan.pdf> accessed 28 August 2023.

[108] The model raises interesting concerns regarding the burden of proof. The assertion to be proved is 'the network and system were not compromised,' and while the modified certificate goes a significant way in proving this, the model essentially relies on the adverse party proving (or failing to prove) that the system or network was

ii: METADATA REQUIREMENTS

The second issue concerns the lack of requirements for metadata in certificates. Metadata is data about data.[109] It refers to information that is automatically generated by the computer and applications.[110] Computer-generated metadata includes data such as last accessed, last modified, date created, author, access rights, location/path, etc.[111] Application-generated metadata can include fields such as edit history, version history, application version used, etc.[112] Furthermore since it is autogenerated by the system, it has a high degree of reliability. Metadata can therefore serve a useful purpose when it comes to digital evidence. As an illustration, the last modified date can inform the judge if the file was tampered with after a critical point in time. This coupled with edit and version history can inform the judge of the exact changes that were made to the file. Additionally, if the date created is after the last modified date, it suggests that the file was copied. This can help trace the provenance of the file and discover evidence of tampering, editing, etc.

From the provisions of the Indian and Malaysian Evidence Act relating to certificates, it is clear that these jurisdictions have little to no metadata requirements. Even case law in these two jurisdictions does not reveal much about the use of metadata in these certificates. In India, the Courts have occasionally commented on the importance of metadata,[113] and in some high-profile terror trials it gets argued,[114] but there is no considered opinion on the use of metadata when it comes to digital evidence. In Malaysia, the lack of metadata, in the context of digital evidence (emails), has been pleaded as a defence and as affecting the authenticity of the evidence.[115] But this was rebutted by a presumption under section 114A(2) of the Malaysian Evidence Act. In

---

compromised. Otherwise, the party producing the digital evidence will have the burden of proving a negative which is generally avoided. This also raises questions in case of criminal trials where the entire burden of proof is traditionally on the prosecution and there is also gross inequality of resources. However, these issues fall outside the scope of inquiry of this paper. Here, it suffices to say that these concerns must be borne in mind when discussing issues of digital evidence.

[109] Schefer and Mason (n 57) [2.22].

[110] ibid [2.24].

[111] Ryan D Pittman and Dave Shaver, 'Windows Forensic Analysis' in Eoghan Casey and ors (eds), *Handbook of Digital Forensics and Investigation* (Academic Press 2010) 231.

[112] ibid 232-235.

[113] *K. Ramajayam v. Inspector of Police*, 2016 SCC OnLine Mad 451 [35]; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1* [73.4].

[114] *State of Maharashtra v. Mahesh Kariman Tirki*, Sessions Case No. 13 of 2014.

[115] *Yusof Holmes bin Abdullah v Public Prosecutor* [2019] MLJU 999.

another instance, metadata was used to verify when certain photos were taken.[116] On the other hand, in Singapore, the Supreme Court Practice Directions specify that metadata should be preserved during the discovery of electronic evidence.[117] An analysis of Australian case law reveals that metadata has played a part in determining the weight that is given to evidence but not its admissibility.[118]

The issue with how metadata is treated in India and Malaysia is that it does not get seriously argued or substantively engaged with. Lawyers and courts are simply not asking the right questions. It is often asserted as a standalone fact to prove its contents, for example, the author of a document or the date of creation of photos.[119] Even where it is argued, the court uncritically examines it.[120] More importantly, it is never treated as a requirement to check the authenticity of digital evidence. Metadata analysis needs to be a routine part of dealing with digital evidence. In Singapore, while the practice directions require that it is preserved, the authors have not come across any court decision that seriously considers metadata of digital evidence. Lastly, while metadata gets raised and argued in Australia, it is at the stage of probativeness and not at the stage of admissibility. This does not mean that metadata is perfect. Metadata is also susceptible to manipulation and can be erased. Many of the metadata fields rely on system information being correct so the time and date of the system need to be correct. This can be problematic when a file is being edited across multiple time zones on a cloud. Because of the model's reliance on an adversarial setup, metadata can prove to be immensely useful in proving the provenance and source of digital evidence.

IV: CONCLUSION

This paper explored the use of digital evidence through the lens of Asia-Pacific Countries and has tried to answer the two major debates that have arisen in this context. First, in the context of varying admissibility requirements of digital evidence the paper explored the question of whether digital evidence should be treated as a separate category of evidence like oral and documentary evidence. The paper answered this in the affirmative by identifying different models of technological

---

[116] *C.A.S v M.P.P.L & Anr* [2022] AMEJ 0748; *Mohd Nashriq bin Ismail & Anor v Public Prosecutor* [2018] 4 AMR 582; *Pendakwa Raya v Liew Kee Sin* [2016] AMEJ 2215.
[117] Singapore Supreme Court Practice Directions 2013, para 52(1).
[118] *ASIC v Rich* (2009) 236 FLR 1.
[119] See (n 116); *State of Maharashtra v. Mahesh Kariman Tirki*, Sessions Case No. 13 of 2014.
[120] *State of Maharashtra v. Mahesh Kariman Tirki*, Sessions Case No. 13 of 2014.

neutrality. The paper differentiated between formal and substantive technological neutrality. It argued that treating digital evidence as a separate category is more in line with the goals of technological neutrality or what has been referred to as substantive technological neutrality.

It then argued that substantial differences exist between digital evidence and other forms of evidence to warrant treating it separately in terms of additional vulnerabilities of electronic evidence along with other features such as process dependency, originality, etc. The paper also looked at the legal ramifications of treating digital evidence as documentary evidence by assessing its viability in the face of the best evidence rule.

Second, the paper attempted to answer the question of how digital evidence should be treated differently. Since the paper is focused on Asia-Pacific countries, it restricted itself to the certification model and explores the differing standards of certification that exist in the selected countries. It compared the nature of certification requirements and argued that Malaysia's approach of allowing either certification or oral testimony makes the most sense. It also criticised the countries' tendency to classify digital evidence as primary or secondary in light of the critique in the first part.

Lastly, it made a normative critique, exploring the inadequacies of the certification requirements, across the models. It noted that the certification models don't account for the decentralised nature of present technology. It argued that in light of the decentralised nature, it made little sense to identify one person who can assure the propriety of the digital evidence and recommended that more actors who have access to the system be identified to verify the assurance given and provide additional information. Further, it also suggested that information about the network to which the system is connected should also be included in the certification requirement.

The paper also suggested the inclusion of computer-generated metadata in the certificates to prove the integrity of digital evidence. It highlighted that while the current models focus on the proper functioning of the device at the time of production of digital evidence, metadata can, on the other hand, provide useful information about the integrity of digital evidence while it is stored on the device. It can also provide information about its provenance. Both recommendations rely on an adversarial system as they depend on providing information to the other party necessary to uncover tampering or pose further inquiries into the reliability of evidence.

The adjustments suggested have been limited to a certification model because of the countries chosen. Further, the model raises interesting concerns regarding the burden of proof. It essentially relies on the adverse party proving (or failing to prove) that digital evidence was compromised. Otherwise, the party producing the digital evidence will have the burden of proving a negative which is generally avoided. This specifically raises questions in the case of criminal trials where the entire burden of proof is traditionally on the prosecution and there is also gross inequality of resources. However, these issues fall outside the scope of inquiry of this paper. Here, it suffices to say that these concerns must be borne in mind when discussing issues of digital evidence.