ELECTRONIC EVIDENCE IN THE HEALTHY JUSTICE SYSTEM: REIMAGINED

Rita Komalasari
Yarsi University, Indonesia
rita.komalasari161@gmail.com

Cecep Mustafa
Stirling University, United Kingdom
cecepmustafa97@gmail.com

Abstract

This study addresses one of the critical difficulties related to the admissibility of electronic evidence. This essay examines the reliability of electronic evidence in foreign criminal and civil justice systems and offers suggestions for revising the reliability of electronic evidence in Indonesian court processes. In terms of the legitimacy of electronic evidence in the criminal justice system, the method adopted is the present comparative policy approach in various nations. The paper presents the concept of a rapid check mechanism for verifying electronic evidence, which swiftly advances the settlement of criminal and civil cases.

Keywords: validity, electronic evidence, admissibility, rapid check mechanism.

Introduction

Electronic evidence has become integral to modern criminal and civil justice systems worldwide, including Indonesia. Utilizing electronic evidence poses challenges and opportunities, particularly concerning its admissibility and reliability in legal proceedings. This essay delves into a critical examination of the reliability of electronic evidence within foreign criminal and civil justice systems and endeavors to provide recommendations for enhancing its credibility within Indonesian court processes.

The admissibility of electronic evidence presents a multifaceted challenge within the realm of justice systems, including the Indonesian one. This study primarily addresses the following key issues: 1. Reliability of Electronic Evidence: One of the foremost challenges in utilizing electronic evidence lies in its reliability. Ensuring that digital data is trustworthy and unaltered is crucial for upholding the integrity of legal proceedings. However, establishing this reliability has been a recurrent issue, leading to skepticism from legal practitioners and the judiciary. 2. Comparative Policy Analysis: This study employs a comparative policy approach to assess the admissibility and reliability of electronic evidence across various nations. This approach helps identify best practices and areas of improvement, allowing us to draw insights from the experiences of other legal systems. 3. Rapid Verification Mechanism: The paper introduces the innovative concept of a rapid verification mechanism for electronic evidence. This mechanism aims to expedite the resolution of criminal and civil cases by streamlining the process of authenticating digital evidence, ultimately reducing case backlog and ensuring timely justice delivery.

The challenge of ensuring the admissibility of electronic evidence is of paramount importance in contemporary legal systems. As society becomes increasingly digitalized, electronic evidence plays a pivotal role in investigations and court proceedings. However, concerns surrounding the reliability of such evidence persist, leading to issues related to the fairness and efficiency of the justice system. Addressing the reliability of electronic evidence is crucial for several reasons: (1) Protection of Rights: Ensuring the trustworthiness of electronic evidence safeguards the rights of both plaintiffs and defendants. Unreliable evidence can lead to unjust verdicts and undermine the principles of fairness and due process; (2) Efficiency and Speed:

Implementing a rapid verification mechanism for electronic evidence can expedite the resolution of cases, reducing the burden on the judicial system and allowing for timely justice delivery.

This essay seeks to accomplish several key objectives: (1) to comprehensively analyze the reliability of electronic evidence in foreign criminal and civil justice systems through a comparative policy approach, and (2) to propose the concept of a rapid verification mechanism as a means to enhance the credibility and efficiency of the Indonesian court processes.

The methodology employed in this study involves a comparative analysis of policies and practices related to electronic evidence admissibility in various nations. This comparative approach allows us to draw on international experiences and best practices. Additionally, the paper explores the feasibility and potential benefits of implementing a rapid verification mechanism within the Indonesian context. This essay contributes novelty to the field by introducing the concept of a rapid verification mechanism for electronic evidence, which has the potential to transform the way electronic evidence is handled in legal proceedings. This essay undertakes a crucial examination of electronic evidence reliability within foreign legal systems, introduces an innovative rapid verification mechanism, and aims to contribute significantly to the discourse on enhancing the admissibility of electronic evidence within the Indonesian court processes. The issues discussed are of utmost importance in the digital age, where electronic evidence holds the key to fair and efficient justice delivery.

Throughout the 20th century, as information technology (IT) evolved and expanded, it began to be implemented into modern courts in various ways. The reliability of electronic evidence in international criminal and civil justice systems is examined in this article, and recommendations are made for improving its reliability in Indonesian court procedures. The approach used is the current comparative policy approach in Europe,[1] American and Japanese countries in terms of a rapid check mechanism for verifying electronic evidence in the criminal justice system.

[1] Hong, Ilyoung. "International Digital Forensic Investigation at the ICC." *Handling and Exchanging Electronic Evidence Across Europe* (2018): 125-139.

The Current State of Electronic Evidence in the Indonesian Justice System

The Indonesian justice system oversees a wide array of civil and criminal cases, each subject to its distinct procedures and rules of evidence. It is within this context that electronic evidence has become increasingly prominent. Electronic evidence has emerged as a powerful tool for law enforcement agencies and the defense in criminal justice. It encompasses a wide range of digital artifacts and data types that play pivotal roles in investigations, prosecutions, and trials. Some of the most common forms of electronic evidence in criminal matters include Digital Forensics. Digital forensics involves collecting, preserving, and analyzing digital data from various sources, such as computers, smartphones, and storage devices. This type of evidence often plays a central role in cybercrimes, financial fraud, and computer hacking cases. Surveillance Footage: Surveillance cameras, both public and private, capture critical evidence in criminal investigations. Footage from these cameras can provide crucial visual evidence in cases involving theft, assault, vandalism, and other offenses. Electronic Communications: Emails, text messages, and instant messaging conversations are frequently used as evidence in cases related to threats, harassment, extortion, and even terrorism. The content and metadata of electronic communications can shed light on motives, connections, and timelines. Social Media Content: With the widespread use of social media platforms, online content, including posts, images, and videos, often serves as evidence in criminal trials. This can include evidence related to threats, harassment, or even admissions of guilt.

While criminal cases harness electronic evidence to establish guilt or innocence, civil matters also benefit significantly from the digital footprint left by individuals and organizations. In the civil arena, electronic evidence commonly includes electronically stored documents. Electronically stored documents, such as contracts, invoices, and financial records, are ubiquitous in civil litigation. These documents are often stored electronically, and their authenticity and integrity are critical in legal disputes. Email Correspondence: Similar to criminal cases, emails are frequently used as evidence in civil matters. They can provide insights into contractual agreements, disputes, and

communication between parties involved in a civil case. Digital Records in Intellectual Property Cases: In intellectual property disputes, electronic evidence may include records of patent applications, trademark registrations, and evidence of copyright infringement, often found in digital formats. Social Media as Evidence: Social media content can be pertinent in defamation cases, employment disputes, and family law matters. Posts, photos, and messages shared on social platforms can provide insights into an individual's behavior and statements. It is essential to recognize that the admissibility and reliability of electronic evidence vary across different case types and contexts within the Indonesian justice system.

In our quest to gain insights into the admissibility and reliability of electronic evidence in the Indonesian justice system, we turn our attention to a theme-based comparison with other countries. This approach allows us to delve into specific aspects of electronic evidence handling, including admissibility criteria, verification mechanisms, and the influence of legal precedents. By organizing our comparative analysis thematically, we aim to provide a clear and concise overview, making it easier for readers to grasp the key differences and similarities.

The Validity of Email

Table 1 summarizes the key points from the text and can serve as a visual aid to help readers grasp the information regarding the validity of emails more easily.

Table 1: Validity Assessment of Email

Challenge	**Considerations**
Authorship of Email	Multiple users per account; unauthorized access
Authentication Evidence	Witness testimony: Defendant's name, frequent usage

The main problem with evaluating electronic email verification's validity is determining the email's author. Bear in mind that more than one person can use an email account. Accessing an email account without the account owner's consent is possible. Therefore, it frequently proves insufficient to determine the authenticity of the

author's identity based on the fact that emails contain specific things in the email address; usually, the Court demands at least a bit of evidence. Required information: the witness can explain that the email contains the Defendant's name and email address, and he often sends emails to and receives emails from those concerned at the email address that appears. There are times when the prosecutor submits email evidence, completed through the victim's testimony, that the victim is aware of the Defendant's email address and has previously received emails from the Defendant. This can be seen from the case of Shea against the United States Government. The whistleblower's statement that she knew Defendant's email address and that she had received emails from Defendant allowed the public prosecutor to verify the authenticity of the communications; as many as six emails were shown at the trial.

The validity of the Website

Table 2 summarizes the key points from the text and can serve as a visual aid to help readers grasp the information regarding the website's validity more easily.

Table 2: Validity Assessment of Websites

Evaluation Criteria	**Details**
Content Verification	Ensure downloaded content matches the original website
Methods of Verification	Internet archive, website owner's/sponsor's testimony
Case Example	Telewizja Inc. vs. Satellite Corp. with Internet Archive usage
Challenges	Verification during legal proceedings and need for witness

Regarding the website, it is the responsibility of the authenticating party to demonstrate that the content downloaded is what was available on the website at the moment (tempus) charged. Utilizing an Internet archive site might be part of the validity evaluation process. Some court rulings seem to mandate or indicate that the website owner or sponsor's testimony is required. Courts in the United States consistently argue that evaluating the validity of a website does not stand alone and, therefore,

requires authentication. When consumers access an older website, this is very important. For example, the case of Telewizja Inc. against Satellite Corp. is a case of a well-known archive website. The Plaintiff tried to demonstrate how the Defendant's website appeared in the past. The Plaintiff uses Internet Archive, a nonprofit with 150 billion online archives. The Plaintiff copied a portion of what was thought to be the Defendant's website on specific dates from an Internet Archive copy. To verify that the page was indeed captured, the Plaintiff submits administrative permission from the Director of the Internet Archive. The Archive Director then confirmed that the Plaintiff's copy of the website matched the web page's appearance in the Archive Internet records. The Court determined that the Plaintiff's proof was adequate justification for authenticating the printed webpage.

On the other hand, the Defendant could not prove otherwise, so the Defendant's rebuttal was rejected, and the Court granted the Plaintiff's claim. In another case between the Laser Institute and Sanderson, for example, Plaintiff attempted to rely on the testimony of two witnesses to establish the veracity of prints obtained from the Internet Archive. However, neither witness was familiar with the Internet Archive. The Court then shrewdly reminded the Plaintiff of the proper way to authenticate printouts from the Internet Archive by obtaining a validation sheet from an Internet Archive representative, stating that he had personal knowledge of its contents and confirming that printouts were correct and accurate in accordance with Archival records, and doing so by stating that he had personal knowledge of it and doing so by confirming that printouts were accurate in accordance with those records.

There are at least three stages of authentication for website material, namely, Knowing the actual content contained on the website. In the United States, this is an essential consideration for judges because the content on the website is dynamic because the work of displaying content is constantly running. During legal proceedings, a person tries to download something from a website. The content that was downloaded might not be the same as what was available online when the item was under scrutiny at trial. In this situation, it is the authenticating party's responsibility to show that the content downloaded is indeed what is available on the website at issue. Hear a witness who can explain that what is contained on the web accurately

reflects. For example, this is evident from the United States Government's lawsuit against Jackson. In this case, the Court believes that there is a need for testimony from the website owner. Furthermore, Jackson, as the website owner, tried to convince the Judge that the posts that appeared on the website were his.

Ensure that the content contained on the website is caused by the owner of the website. For example, This is evident from the Case between Costa and Keppel Ltd. The Court did not find adequate party testimony that could explain that the witness had visited the website operated by the enemy. The Court also did not find any testimony from representatives of Keppel Ltd., which could prove the Court declined to take the information into consideration since Keppel Ltd. posted it on the internet. This is needed to anticipate the existence of a well-publicized hacking incident that can trigger judges' doubts. There's a chance that the content on the website wasn't created by the website's owner or sponsor. For instance, occurrences of hacking are a problem in the United States that is most often the focus of the Court.

The validity of Text Messaging, Social media posts

The following table 3 summarize the key points from the text and can serve as a visual aid to help readers grasp the information regarding the validity of text messaging, social media posts more easily.

Table 3: Validity Assessment of Text Messaging and Social Media

Evaluation Aspect	**Considerations**
Authentication of Messages	Screenshots; potential issues with edited content
Case Example	Dispute between the United States and Defendant Jackson
Identifying Senders	Challenges with identifying senders in social media
Witness Testimony	Importance of lay witness testimony

The validity assessment is related to the reception of messages and texts, social media posting requires searching about the identity of the

sender of the message and the accuracy of the communication.[2] Usually, the Court feels that it is sufficient to stipulate that screenshots of Instant Messages, Texts, and social media posts that are shown at the trial are the result of communication with adequate accuracy. However, sometimes, problems arise when the conversation has been edited. The dispute between the United States and Defendant Jackson serves as one such. The Defendant was charged with attempting to coerce a youngster into having sex. The government agent, who pretended to be a fourteen-year-old girl, had an online communication with the Defendant, and the public prosecutor attempted to include a copy of that conversation. The Public Prosecutor felt that the transcript of this conversation was the only version of the government to document what the Defendant had done to the government agency. During the trial, on the one hand, the Court found that the version of the conversation presented by the Public Prosecutor was inaccurate: there were many examples of missing data, there were some timelines that didn't make sense, and agents added their own editorial information. On the other hand, Jackson's opinion cannot be read; however, it is an indication that the cut-and-paste version of an online chat or anything less than the entire, unedited original will be immediately excluded by the Court in this case. The Court must determine if further proof is sufficient to demonstrate that the provided exhibits accurately represent what he meant in the indictment.

Problems that often arise in the validity assessment are related to the receipt of messages and texts. The purpose of social media posting is to establish the actor's identity testimony from people with firsthand experience about the perpetrators' identities, which is often difficult to obtain. Perpetrators who are suspected of having good conversations through instant messages and social media posts are usually only identified by the name printed on the communication device screen. There isn't always a verbal or sight touch to identify someone. In other situations, the Court ruled that a witness's personal knowledge might be used to authenticate documents. These had to do with how the witness discovered the actor's identity or how the witness's personal information appeared to fit the definition of a lay opinion as defined by

[2] Flanagan, Elizabeth A. "# Guilty: Sublet v. State and the Authentication of Social Media Evidence in Criminal Proceedings." *Vill. L. Rev.* 61 (2016): 287.

the Regulations. Examples of disputes between Defendant Hunter and the US Government. Assume that the Court stated that the text message shown to the Defendant was justified by the Defendant, in other cases between the United States Government and Defendant Bell. In this case, the Defendant was charged with various acts of inappropriate sexual behavior with foster children. In the case, the Public Prosecutor presented one of the Defendant's victims with the opportunity to authenticate copies of the MySpace online chat that the victim and the Defendant had. The Defendant in this case was accused of engaging in a number of improper sex actions with foster children. In the case, the Public Prosecutor showed one of the Defendant's victims in order to verify copies of the victim and the Defendant's MySpace communication. The victim knew the Defendant's MySpace login, and the communication contained code terms that were only known by the Defendant and the victim, according to the Public Prosecutor, who claimed that the victim would be able to identify the Defendant from his online conversation. The Court utilizes the kind of testimony allowed by the Regulations in this particular situation. Types of lay witness testimony that take the shape of findings or views and are based on the witness's own understanding. However, most of the time, text messages, instant messaging, and chat room dialogues need to be allowed using other methods.[3]

A case for digital photography

The following table 4 summarizes the key points from the text and can serve as a visual aid to help readers grasp the information regarding the validity of digital photography more easily.

Table 4: Validity Assessment of Digital Photography

Criteria	**Explanation**
Types of Edits	Distinguishing between "edited" and "enhanced" photos
Witness Testimony	Requirement for a witness to confirm accuracy

[3] Hlavka, Heather R., and Sameena Mulla. "That's How She Talks": Animating Text Message Evidence in the Sexual Assault Trial." *Law & Society Review* 52, no. 2 (2018): 401-435.

Enhanced vs. Edited	Differentiating between enhancements and edits

The development of digital photography and the ease with which software may be used to modify digital photographs have made determining the veracity of electronic documents more challenging. There is diversity around the use of digital photo change vocabulary. Some contend that digital change may come in many different shapes and sizes, including modifying the format, the colors, the filtering, the interpolation, the cutting, the resizing, the reshaping, the covering, the cloning, or the touching. Digital editing of a photo doesn't have to alter the topic it depicts. It's possible to change the subject and give an erroneous description using a digital change. Therefore, it is important to distinguish between digital photographs that have just been "edited" and those that have been "upgraded" when determining the legitimacy of digital photos. In this paper, "digitally enhanced photos" means that the photos owned have been altered in such a way as to make apparent portions of a picture that were previously hidden from view. Digital adjustments can be used to improve the image, specifically to represent what is possible. By enhancements in the condition of the human eye, we cannot distinguish them. Digital enhancements for fingerprint photos have been used, for example, to identify forensic data. The owner of a fingerprint finds patterns that were not previously detected.

The Court requires the testimony of at least one witness who can explain that he knows the picture is displayed and that the location or person at the moment is proportionately and precisely shown in the picture. That has been charged. There are some views that argue that because digitally enhanced photos reveal something that was previously invisible, it must be clear that it cannot be endorsed only by the testimony of a lay witness but requires expert testimony. In the condition that digital photos have been "improved," witness testimonies are needed, which can complement the information that the "enhanced" photos have fairly and accurately described what he meant. In other words, for improved digital photos, the witness's statement was not enough to see the enhanced photo and stated that The witness was familiar with the situation captured in this photo, and it was correctly and fairly captured. Witnesses who have firsthand experience with the methods used to create digitally enhanced photographs and can attest

that these methods are utilized to create enhanced images and preserve their correctness must provide further testimony. As long as digital photographs aren't improved, a witness with personal knowledge testimony—that is, a statement that the witness understood the visuals exhibited in the photograph fairly and properly portrayed the scene or the subject at the relevant time—could prove its authenticity. These also apply to photos that are altered (but not digitally - "enhanced"). Including photos of films that have been enlarged, trimmed, or changed in contrast is clearly considered fair for cross-examination. This is usually considered authentication by the witness's testimony with personal knowledge. For this reason, technical guidance is required for judges to disclose any digital changes other than those permitted by the Regulations. In creating this technical guidance, it should be emphasized that just because an image satisfies the minimum requirements for authentication does not mean that the Court will get it or, if it is, that the Court will find it believable.

The validity of animation and computer simulation

The following table 5 summarizes the key points from the text and can serve as a visual aid to help readers grasp the information regarding the validity of animation and computer simulation more easily.

Table 5: Validity Assessment of Animation and Computer Simulation

Criteria	Description
Computer Animation vs. Simulation	Differentiating between animation and simulation
Validity Assessment	Considerations for assessing the accuracy of simulations

The difference between computer animation and computer simulation is parallel to the difference between digital images that aren't altered and regular digital photos. According to one Court, data is input into a computer that is configured to assess data, do calculations using scientific principles, draw conclusions, and replicate case occurrences during a simulation. To put it another way, computer animation is just a collection of pictures created by a computer that acts as a road map. For instance, it might explain what witnesses saw or provide evidence

of an expert's perspective of how an event happened.[4] Considering the examples above, the Judge can make a validity assessment.

In conditions where proof requires the production of electronic documents that are very much from the original, then for the purpose of presenting a sample of electronic documents at the time of proof at a hearing, there is a need for technical regulations to be made to provide exceptions to the rules when the original documents are very large. Under Rule 1001 (3), concerning Evidence in US justice. An original document consists not only of data stored electronically but of printed output or another clearly visible output that appropriately reflects the data shown. Therefore, any printed data that correctly reflects the data qualifies as an authentic business record when a firm maintains data in a manner that complies with the business requirements records exclusions. Instead of requiring enormous production of original electronic documents, parties are allowed to appropriately describe their contents and provide those summaries to the Judge. Printouts from summary business documents tend to be simpler for plaintiffs in the US to consider and examine. It makes more sense, in a way, to refer to such content as a summary. Furthermore, the fact that it is being treated as a summary should not influence whether it is acceptable as long as the parties adhere to Rule 1006's basic standards regarding proof in the United States.[5] The rules for presenting this summary are exceptions. This exception seems to be very much in line with the benefits of using computers. Computers have the capacity to gather and summarize common facts from very big document files, which is one of its benefits. Typically, the Judge is merely given a sample of the printed and assembled information. However, this does not imply that what is sent to the Court is flawless evidence because it is only a summary. This enables parties with plaintiffs to utilize extremely comprehensive summaries of electronic documents as long as the original or copies of such documents are accessible to other parties for viewing or copying

[4] Dyrda, Adam, and Maciej Próchnicki. "Expert's (Meta) Testimony: An Epistemological Perspective." In *Theory of Legal Evidence-Evidence in Legal Theory*, pp. 169-188. Cham: Springer International Publishing, 2022.

[5] Novak, Martin. "Digital evidence in criminal cases before the US courts of appeal: Trends and issues for consideration." *Journal of Digital Forensics, Security and Law* 14, no. 4 (2020): 3.

at a reasonable time and location. Technically, there is no question whether the manner in which the firm actually configures and uses the data in everyday business operations is taken into account when printing the data. If necessary, electronic data printed for litigation purposes can be configured to meet the requirements as original documents for proof of trial as long as the printing faithfully reproduces the electronic data. Let's say a company tracks all sales using a computer, publishes reports on a regular basis, and utilizes monthly sales reports for each area. For trial purposes, businesses strive to explore electronic data more profoundly and print monthly sales reports that are made per regional postcode. The data from which the report was produced fulfills the requirements of electronic documents at the trial as long as the parties can show that the sales-with-postal code report accurately reflects that data, the report qualifies as original documents for the purpose of proof at trial.

The validity of electronic evidence in Japan

The following table 5 summarizes the key points from the text and can serve as a visual aid to help readers grasp the information regarding the trustworthiness of electronic evidence more easily.

Table 5: Electronic Evidence Handling in Japan

Aspect	**Key Points**
Legal Framework	No integrated laws for civil and criminal procedures
Freedom of Judgment	Judges have the freedom to evaluate evidence based on credibility
Electronic Records	Computer data treated differently due to verification challenges
Authentication of Docs	Electronic documents with electronic signatures are considered authentic
Handling Electronic Data	Importance of printouts for checking evidence
Discovery and Disclosure	No formal discovery or disclosure

In this paragraph, the principle of evidence in civil procedure is discussed. In Japan, there are no integrated laws for civil and criminal procedures. Both procedures have separate provisions relating to the examination of evidence. In Japan, the principle of freely evaluating evidence is the principle that gives judges freedom of judgment to determine the legal facts that are fundamental to the Court in civil and criminal procedure.[6]

In civil procedure, there is no limit to the receipt of evidence except for evidence collected illegally. The judge can, at his discretion, determine the basic facts to take the court into consideration during the entire trial process. The Judge can also consider the attitude taken by a party, such as delays in making documentary documents, as a factor towards those parties.

Both civil procedure and criminal procedure have general provisions for examining electronic evidence.[7] Civil procedures provide the possibility of receiving audio and video recordings as evidence, quasi-proof documents, but according to the purpose of the lawmaker, it is not intended to cover computer data. Computer data (digital data) is usually treated differently from audio recordings and video tapes (analog data), because the contents cannot be verified directly using a playback engine and there is no single media or form.

There are three main reasons why there are no specific provisions relating to electronic records as evidence. First, based on the idea that you may evaluate evidence in any way you like, it can be accepted in civil litigation, but do an assessment based on its credibility. Second, in practice, the Court does not need special provisions to examine an electronic record. It is assumed that a judge can examine electronic records either by examining printouts as documentary evidence, through expert witnesses, or in the selection of media that store information. For these three reasons, there are difficulties in compiling general provisions that cover a variety of media in a comprehensive manner. Official documents are considered authentic, and personal

[6] Kaneko, Hironao. "Electronic Evidence in Civil Procedure in Japan." Digital Evidence & Elec. *Signature L. Rev.* 5 (2008): 211.

[7] Bungert, Maximilian. "Do It for the Snap: Different Methods of Authenticating Snapchat Evidence for Criminal Prosecutions." U. Ill. *JL Tech. & Pol'y* (2021): 121.

documents signed or sealed by the author or the author's representative are deemed authentic. The Court can accept or reject the presumption of the authenticity of these documents. Electronic documents cannot be physically signed or sealed. Thus, the criteria for assuming the authenticity of documents, that is, the existence of a signature or seal attached to the document, do not apply to electronic documents. Legal provisions related to certification that utilize electronic signatures are intended to resolve the issue. Article 3 states that electronic documents with electronic signs affixed by the author are considered authentic.

In civil procedure, a document that is presented as evidence must be original. However, an official copy of the document or the document's original copy can be accepted as a substitute. With this rule, it can be assumed that electronic data recorded in the media can be considered genuine. Some courts at the first level consider electronic print data to be authentic because the electronic data itself cannot be signed.

Printing notes are the most important material for checking electronic records that are stored as evidence. According to the eclectic examination method, the media that stores the data, as well as print results, can be submitted to the Court as quasi-proof documentation. The party requested to produce electronic records on the storage media must provide additional information, such as the name and whereabouts of the operator responsible for entering data into the media, as well as the details of the operator that produced the prints, software, and record formats needed for which content checks and electronic records. If the party requested does not disclose such additional information, the Judge can determine, based on the appraisal of the free evidence concept, that the party is expected to provide the evidence that the Court as a whole requires unless it shows a justifiable reason.

It is crucial for specialists in the field of digital evidence to analyze or inspect the media itself if the validity of the data or the identification of printouts and data contained in the media is a concern. The Court can also contact the electronic registry operator to appear in Court as a witness.

In Japan, there is no discovery or disclosure, unlike in the United States or Britain. Civil Procedures in Japan provide several categories of documents that must be made to the Court. It states the responsibility

of the parties to produce documentary evidence to the Court. The production sequence for the production of documentary evidence usually applies to printed, electronic records that are available at the time of the hearing for proof examination. The parties who will present the electronic document must attach the title, summary, source name, facts to be proven, and the basis of the argument related to the evidence.

In court practice, through discussions between the Judge and the parties, when clarifying and focusing on the initial stages of the trial procedure, the parties are reminded or asked to present evidence in Court. A judge can consider the failure of a party to cooperate as a factor in the consideration of the decision, in addition to the evaluation of the evidence presented by the parties. If the parties produce documents that violently violate, then the Court can decide against that party. However, it does not affect the existence of sanctions against the parties, such as contempt of the Court.

In Japan, it seems that the Court does not consider it necessary to examine the enormous volume of electronic information storage. The Court may ask one of the parties to make a summary or part of the results of the electronic information storage that is shown by the parties without submitting the entire copy of the electronic information storage to the Court. If there are objections to the authenticity of the electronic information storage summary, the Court may ask the parties to produce an additional print from the electronic information storage, or the Court will check the electronic information storage.

In Japan, a small number of case reports published there mention related to the procedure for submitting digital proof. Examining electronic evidence is frequently required in several case types, such as harassment cases, lender lawsuits, trade cases, and medical malpractice claims. In trade cases, the Court, in practice, asks fined traders to create charts that trace the history of transactions with customers in tabular form and produce them in electronic format. This is intended to clarify the problem in the case. However, even in this case, printed electronic documents must be checked.[8]

In recent years, there have been many consumer cases suing lenders, claiming reimbursement, including interest that exceeds the

[8] Kaneko, Hironao. "Electronic Evidence in Civil Procedure in Japan." Digital Evidence & Elec. *Signature L. Rev.* 5 (2008): 211.

limits given by the Interest Restrictions Act. In these cases, the consumer, as the Plaintiff, starts the proof by collecting transaction records for ten years, which are stored in the Defendant's computer system. Defendants, as money lenders, repeatedly refused to make the record.

The appeals court concluded that the Defendant did not show sufficient evidence that the Defendant's computer system routinely deleted records for ten years and was inconsistent with the statements in the previous customer's case. The verdict handed down in Court wins the consumer. There are problems in obtaining electronic evidence from backup records and post-disaster recovery, which means they need to be recovered so that data can be read. However, there are no rules related to whom costs are charged in data recovery.

Europe Union's concept of a rapid check mechanism for verifying electronic evidence

The acceptability, legitimacy, correctness, and integrity of electronic evidence must be assessed in the same ways as traditional forms of evidence. The handling of electronic evidence must be to the harm of the parties or provide any of them an undue advantage.

The verbal proof was obtained over a distant link. If the nature of the evidence permits, spoken evidence may be obtained remotely utilizing technological tools. The Court must specifically take into account the following factors when determining whether oral evidence can be taken remotely: the significance of the evidence; the status of the person providing the evidence; the security and integrity of video links through which evidence will be sent; the costs and challenges of prosecuting relevant parties. When gathering testimony from a distance, it is important to make sure that (a) everyone involved in the trial and bystanders in the community where the trial was held in a public place can see and hear the transmission of oral evidence and (b) people heard from remote locations can see and hear the process to the extent needed to make sure that they are carried out fairly and effectively. (c) The methods and technologies used to gather evidence from distant places are carried out in a way that preserves the admissibility of the evidence and the Court's capacity to identify the party in question. (d) Whether the evidence is supplied through a public or private link. To prevent

interception, the video transmission must be encrypted, and the video conference must be secured.

The mere fact that evidence was gathered and/or delivered electronically does not give the Court the right to reject it or to question its validity. In general, a court cannot dismiss an electronic piece of evidence as inadmissible because it lacks sophisticated electronic signatures or other equivalent safeguards. The importance of metadata and the potential repercussions of not using it must be understood by the courts. There must be no requirement for printouts, and the parties must be allowed to present electronic evidence in its original electronic format.

A trustworthy service must be used to gather electronic evidence in a proper and secure manner and to present it to the Court. States must adopt protocols for the secure seizure and collection of electronic evidence because there is a larger danger of harm or loss to electronic evidence than to non-electronic evidence.

To increase litigation efficiency, the supply of electronic evidence must be supported and promoted. Electronic evidence must be able to be sent using systems and equipment that can keep its integrity. To prevent an overwhelming number of requests for electronic evidence, the Court must be actively involved. In cases involving complicated evidentiary concerns or allegations of evidence manipulation, courts may order specialists to analyze electronic evidence. Whether the person has sufficient knowledge of this subject must be determined by the Court.

The following Table 6 summarizes the key points from the text and can serve as a visual aid to help readers grasp the information regarding the trustworthiness of electronic evidence more easily.

Table 6: Trustworthiness of Electronic Evidence

Aspect	Factors for Consideration
Electronic Signatures	Various types and their legal implications
Metadata	Importance in evaluating the context of electronic evidence
Preservation	Methods to ensure data integrity and accessibility

Migration	Strategies for transferring data to new storage media

Trustworthiness

The Court must take into account all pertinent information regarding the origin and veracity of electronic evidence when determining whether it is reliable. Electronic data is admitted as evidence at the Court's discretion unless either party challenges the data's veracity. Unless and until there is a reasonable question to the contrary, electronic data is regarded as reliable if the integrity of the data can be safeguarded and the identity of the signer can be verified. Special protection must be provided by the applicable legislation for vulnerable groups of individuals. If the public service provider's authority sends electronic evidence without the involvement of the parties, the evidence's contents are conclusive unless and until it is shown differently.

Legibility, accessibility, integrity, authenticity, trustworthiness, and, if needed, secrecy and privacy must all be maintained when storing electronic evidence. It is necessary to store electronic evidence with standardized metadata in order to make the manufacturing context obvious. It is necessary to periodically ensure that stored electronic evidence can be read and accessed, keeping in mind information technology advancements.

Filing of electronic evidence

All safety criteria for electronic records must be met, as well as assurances of data quality, integrity, confidentiality, and authenticity. Electronic evidence archiving requires the expertise of experienced professionals. To retain access to electronic evidence, data must be moved to another storage medium as needed.

According to the first principle, the Court must ultimately determine the potential value of evidence derived from this form of evidence, even though the participation of specialists in the appraisal of electronic evidence is crucial. Consequently, presumptions of relevant law may bind the Court (for example, providing specific evidentiary values for certain types of electronic evidence).

The second principle emphasizes that electronic evidence cannot be treated differently than other forms of evidence or given special

treatment. The Court in this instance must also take a disinterested stance toward technology. Therefore, it is necessary to embrace any technology that can demonstrate the veracity, correctness, and integrity of data.[9]

The third principle deals with the fair handling of electronic evidence in regard to the trial's parties. Parties to civil or administrative procedures should not suffer as a result of how electronic evidence is handled. For instance, if the Court only permits one party to submit electronic evidence in printed form, that party must not lose the chance to send pertinent metadata to support the validity of the printout. Another example would be that a party must not lose the chance to contest the authenticity of electronic evidence.

Spoken testimony recorded via a remote connection

Electronic evidence is regarded to be original evidence obtained through a distant link. However, it does not include previously recorded oral evidence. This is related to oral evidence in the form of video conferencing (transmitting images and sounds that are synchronized in the present). Not all oral testimony can be obtained through a remote link. The technological equipment used to convey spoken evidence requires attention. Using analog or digital technological tools that enable telecommunications transmission, particularly real-time two-way communication that permits the transfer of pictures and sound, may be done remotely. If testimony must be kept private, it can be essential to put in place technical safeguards or solutions to restrict access to secure channels of communication that are only understandable by authorized parties. Telecommunications integrity will give courts and parties adequate and appropriate opportunities to refute and question "long-distance" witnesses.

Economic factors (such as a decrease in expenses), logistical challenges (such as a witness's illness or incapacity), and procedural efficiency measures to avoid a lengthy procedure are what determine whether oral testimony is obtained through long-distance interactions. It could be more suitable to inquire remotely if the person is located somewhere else. The same rule applies to a group of witnesses who are

[9] *See* European Court Ruling for Human Rights case between García Ruiz against the Spanish Government, No. 30544/96, paragraph 28.

present to hear the case but whose homes are located beyond the Court's jurisdiction. Suppose the choice is between in-person witness and distant testimony. For instance, it might be challenging to observe and comprehend the attitudes of distant observers. It should be taken into consideration during the procedure if remote testimony is offered. When evidence is crucial to the outcome of a case, it is crucial to make sure that the technology being utilized enables questions to be asked when witnesses give testimony (assuming there are procedural norms in place). This criterion cannot be satisfied if the transmission is distorted because of poor connectivity or if the parties have restricted access to technological tools. One side could get an unfair advantage as a result. Remote evidence must be collected in the same way as when presented to trial, to the extent that is technically practicable. The technique employed must adequately protect the transmission of pictures or sound from loss, distortion, or illegal disclosure. By ordering the witness to present the necessary documentation, such as an identification card, passport, or current driver's license, the Court can confirm the witness' identity.

Public and private communication channels must both be used to guarantee video conferencing quality and minimum video signal encryption to protect from intrusion and eavesdropping. It is possible to receive evidence through personal connections, If national law allows, as long as the chosen solution provides enough technological security and abides by procedural protections. In this sense, a "personal connection" refers to a system of unofficial communication or a form of governance designed expressly to collect evidence for legal proceedings.

Using digital evidence

If printed, electronic evidence is presented, the Court may direct the relevant party to include the provisions of the original electronic evidence at the request of one party or on its own initiative. Geolocation information is one example of evidence that, if supplied in its original form, may be crucial in resolving disputes.[10]

[10] See Croatian Supreme Court Decision (case No. I- 696 / 04-7) which confirms SMS texts are a source of information comparable to other textual content kept in other media, thus they may be used as evidence in the process.

Technologies that will be used to safeguard evidence on a blockchain, for example. A new technology called blockchain has the potential to improve the security and reliability of electronic evidence. The term "distributed ledger" can be used to describe a collection of records (blocks) that are kept in a decentralized peer-to-peer network, connected together, and safeguarded using encryption. By design, the blockchain is naturally resistant to data tampering. Data recorded in a block cannot be altered retrospectively without also altering all blocks that come after it, which requires majority network consent. This makes the blockchain suitable for proof purposes. For example, in the US, rule number 1913 of the Vermont Rules of Evidence reads: Digital records electronically registered on the blockchain must be self-authenticated in accordance with Vermont Rule of Evidence 902 if they are accompanied by a written declaration from a qualified person, made under oath, stating the person's qualifications to certify and: (a) the date and time the record was entered into the blockchain; (b) the date and time the record was received from the blockchain; and (c) that the record was entered into the blockchain, received from the blockchain and that it was received from records are stored on the blockchain as activities that are carried out regularly; and (d) that the notes were made by activities carried out regularly as routine exercises. In China, in its June 28, 2018 ruling, the Hangzhou Internet Court ruled that in previous cases. Data kept on a third-party blockchain platform was sufficiently trustworthy and free from interference to be relied upon and recognized by the Court as evidence in intellectual property disputes.

In current practice, most of the data is electronic do not have sophisticated or high-quality electronic signatures, with no other form of assurance. Electronic signature refers to an electronic signature that satisfies the following criteria: (a) is uniquely associated with the signatory; (b) he is able to identify the signatory; (c) is created using electronic signature-making data that can be signed by the signatory, with a high degree of trust, under his sole control; and (d) signed in such a way that any subsequently introduced changes to the data can be recognized. Eligible electronic signatures refer to complex digital signatures that have been produced specifically for this purpose by specific hardware. This (eligible electronic signature-making tool)). The device must be protected by certificates that satisfy the specifications for electronic signatures, i.e., certificates issued by natural persons or

legal entities that are qualified to provide one or more trust services (trust service provider conditions) and who have been given the go-ahead by the relevant regulatory body. However, they must still be taken into account by the Court as electronic evidence (even though the value of evidence can vary depending on the specific type of case), taking into account, for instance, the various trust services related to managing electronic documents and identifying signatories that are available globally. One illustration is the biometric signature, a technique for producing an electronic copy of a handwritten signature in which a person signs their name using a biometric sensor. The biometric signature may be accepted by the Court as being comparable to a handwritten signature on paper, depending on the relevant statute.

It is common for electronic evidence to include metadata, and the Court must be informed of the evidence's potential usefulness. Similar to how postmarking gives the context for assessing ordinary letters (paper) and their contents, metadata offers the context required to evaluate evidence (data). Data on devices that create electronic evidence, as well as date, time, length, and kind of evidence, may all be tracked and identified using metadata. Relevant metadata, either as direct evidence or as indirect evidence (for example, by displaying the document's most pertinent version) (for example, if data files are manipulated). According to the Irish Court, one of the parties involved in civil actions must inform the other party (or parties). When applicable, electronically saved evidence that includes (metadata) metadata from original documents.[11]

Collection and delivery

Electronic evidence is fundamentally brittle and is susceptible to incorrect treatment, scrutiny, and destruction. Because of this, extra care may be taken to gather this kind of evidence correctly. Failure to do so may render it useless or result in incorrect findings. In civil and administrative proceedings, the parties are often in charge of gathering pertinent electronic evidence. Different data kinds could call for various data-gathering techniques. The integrity of the electronic evidence must not be harmed by measures made to safeguard and gather it. In really

[11] *See* Court Decision between Sretaw v. Craven House Capital PLC (2017) IEHC 580; Gallagher v. RTE.

crucial situations, the parties should think about gathering electronic evidence with the aid of IT professionals or notarial services. Judges must be aware that network-based services are frequently used to store data. This is cloud service delivery.

It will be difficult or impossible for the Court and other parties to handle a large volume of needless electronic evidence that may be produced too easily by one side. Therefore, it is crucial that the Court actively manages electronic evidence with the goal of restricting its use to what is actually required to reach a decision. Active data management must adhere to the proportionality principle. Every request for the production of electronic evidence must be evaluated in light of that evidence's suitability for use in court proceedings, and the parties must have the option of objecting to the request.

Reliability of electronic evidence

The trustworthiness of evidence may suffer if physical identification and digital identity are separated. The creator of the electronic data must be identified by the Court. The identity of the document can be established objectively, such as by an electronic signature or by looking up the email address that provided the document, if the applicable legislation does not stipulate how to do so.

Reputable businesses can offer technical safeguards that ensure the validity of the evidence. For instance, data integrity and authenticity can be ensured through certificates for electronic signatures, often known as a person's digital ID. The Court may request a declaration from the service provider connected to an electronic signature if the signer's identification is disputed. The timestamp (time certification) might be equally crucial in demonstrating the reliability of electronic data. A technology that enables the validation of data integrity is time-stamping. This demonstrates that the data was accurate and unchanged at a specific time. Timestamps are valuable aspects of electronic evidence because they include relevant metadata about the time of their manufacture.[12]

When a disagreement arises, the parties usually agree on the subject that needs to be resolved; thus, the Court is not required to bring

[12] Rijavec, Vesna, and Tomaž Keresteš, eds. *Dimensions of evidence in European civil procedure*. Kluwer Law International BV, 2015.

up the topic on its own initiative until one party raises the problem of the validity of electronic evidence. Parties that want to rely on electronic evidence may be required to demonstrate its validity, such as by supplying metadata or requesting the proper court orders to gather more information, such as trust service providers - only where parties challenge electronic evidence.[13]

As with other types of evidence, one party to a trial can oppose electronic proof. In certain situations, the party may seek the Court to remove evidence, for instance, because the data's creator cannot be accurately identified. Any technique of identification that ensures data integrity can be used to demonstrate the dependability of electronic data, such as certified electronic signatures. However, a decision must be made to determine the legal implications of electronic signatures. For instance, it could be decided that only electronic signatures that meet the requirements must have legal implications equal to those of a handwritten signature (wet ink), or it could be decided that the device used to produce the signature must be under the sole control of the trusted. Examples of certain special trust services kinds that are offered nationwide in varied jurisdictions are trustworthy profiles (Poland), electronic archiving and digitalization (Belgium), information/documents for long-term preservation, and the LEXNET Platform for information exchange between the Judiciary Agency as well as various legal operators (Spain).

Electronic signatures that meet European Union requirements.[14] Courts are not required to conduct special analyses of the technology used to create valid electronic signatures in order to assure data integrity. It is sufficient to look through the list of reliable trust service providers.

Rules relating to the burden of proof. Consumers and vulnerable individuals, such as children, might not be able to offer electronic

[13] Tran, Quynh Anh. "Basic Issues of Evidence and Electronic Evidence in Civil and Commercial Dispute Resolution." In *Electronic Evidence in Civil and Commercial Dispute Resolution: A Comparative Perspective of UNCITRAL, the European Union*, Germany and Vietnam, pp. 51-87. Cham: Springer Nature Switzerland, 2022.

[14] Tran, Quynh Anh. "The Significant Types of Electronic Evidence." In *Electronic Evidence in Civil and Commercial Dispute Resolution: A Comparative Perspective of UNCITRAL, the European Union, Germany and Vietnam*, pp. 89-113. Cham: Springer Nature Switzerland, 2022.

evidence due to technical or financial limitations. These rules are applicable if they are supported by legal provisions that lessen or reverse the burden of evidence. In instances involving vulnerable parties, the Court must take an active role. It is important to respect the value of public (official) electronic evidence production systems. Data from an electronic public record, for instance, can be viewed as official documentation and is thus trusted. Electronic records from other procedures are free from the possibility of human mistakes and may be accepted as trustworthy representations of the facts (for example, when compared to content dictated to the protocol by the Judge).

Electronic evidence retention and storage

Storage in the context of this policy refers to holding information while the relevant civil or administrative process is ongoing. Courts may save electronic evidence on portable devices (memory cards), servers, backup systems, or other data storage devices (including cloud computing). In compliance with current legislation, electronic evidence must be preserved in its original format (i.e., not as a print). Courts must take proactive measures to safeguard the integrity of electronic evidence against risks from the internet, such as damage or unlawful access, by taking into account internet security problems. Courts can avoid the danger of the online world compromising the reliability of electronic evidence and lower security concerns by concentrating on prevention. Electronic evidence may not be made available to unauthorized parties, regardless of the technique employed for storage.

Electronic records that have been stored can be connected to standardized metadata that demonstrates the circumstances of their creation and their connections to other electronic records. A certain level of uniformity in the archiving of electronic evidence is ensured by the adoption of international standards for metadata. The creation of uniform information may be challenging and time-consuming; thus, courts might make use of technologies that facilitate this process. Examples of metadata standardization techniques. There are several tools available to create standardized metadata. For instance, a program for managing metadata can produce XML (eXtensible Markup Language) files with metadata related to digital evidence. Advanced professional software is not necessary to open an XML file. This is a common format that may be used in many different information

systems since it is adaptable. This instrument can make the retrieval and storage of electronic evidence simpler. In this situation, it is necessary to adhere to any applicable international standards for metadata that have been made public by groups like the International Organization for Standardization (ISO).

Filing of electronic evidence

Technical filing requirements and a retention term are often provided by national legislation. The archiving system must be secure and ensure recorded usage and privacy protection. To guarantee the preservation of electronic evidence and to prevent illegal access, the proper technological and organizational steps must be adopted. If utilized, electronic data carriers must have an identity certificate with their fundamental information. The carrier must be well safeguarded, particularly from loss, hazardous chemical reactions, heat, light, radiation, magnetic fields, and mechanical injury. Freight forwarding services can confirm that electronic evidence is being preserved by trained specialists or competent organizations and that data has not been tampered with by them, possibly utilizing electronic signatures or other electronic techniques. It is necessary to correctly preserve both the data on the electronic signature that was used to sign the electronic document and the data used to confirm the signature.

Migration refers to switching the store medium to retain the accessibility of electronic evidence. Missing out on migration might prevent data from being read. Periodic data transfers from one storage medium to another storage medium or from one format to another can be used to archive electronic documents. Metadata pertaining to electronic documents that have been archived must also be migrated. Periodic migration to new storage media is required, taking into consideration factors like deterioration and wear in the media before it becomes unusable owing to technical advancements in hardware and medium. Given technical advancements, migration to a storage medium or new formats must be conducted, if necessary. CDs, DVDs, and other optical discs become unreadable owing to physical or chemical deterioration, which is an example of an outmoded solution. The reasons range from physical abrasions and abrasion of the surface or edge of the disk, including apparent scratches, to the kind of interaction with other impurities. The reflective layer can also oxidize. Long-term

resolution examples: Data can be moved from network devices to cloud computing, for example. As a consequence of technical advancements in the media and hardware, this gadget keeps getting better. Cloud archiving can also provide the user with more cost control because the user just pays for their space use.[15]

Opportunities and Challenges for Adaptation in Indonesia

While the opportunities for enhancing electronic evidence practices in Indonesia are promising, there are several significant challenges and obstacles that must be acknowledged and addressed for successful implementation. These challenges encompass legal, technological, and cultural factors, and they pose complex hurdles for reform. Indonesia currently lacks comprehensive legislation specifically tailored to electronic evidence. The absence of clear legal provisions regarding the admissibility, authentication, and preservation of electronic evidence can create uncertainty and hinder its acceptance in Court. Developing and enacting robust electronic evidence laws that align with international standards is a prerequisite for effective reform.A considerable challenge is the state of technological infrastructure in Indonesia, particularly in remote areas. Uneven access to reliable internet and technology resources may limit the ability of individuals and courts to handle electronic evidence effectively. Bridging the digital divide and ensuring that all stakeholders have access to the necessary tools and training is essential. Electronic evidence often involves sensitive personal or confidential information. Ensuring the privacy and security of this data is paramount. Indonesia must establish stringent data protection laws and cybersecurity measures to safeguard against unauthorized access, data breaches, and tampering. Striking a balance between access to evidence and data privacy is a complex challenge. A significant cultural and technological hurdle is the varying levels of digital literacy among legal professionals, judges, and the general population. Effective utilization of electronic evidence requires a solid understanding of digital tools and processes. Comprehensive training and education programs are essential to bridge this knowledge

[15] Bergman, Kristin. "Cyborgs in the courtroom: The use of Google Glass recordings in litigation." *Richmond Journal of Law & Technology* 20, no. 3 (2014): 11.

gap.Cultural resistance to change can impede the adoption of electronic evidence practices. Legal professionals and judges accustomed to traditional paper-based processes may be hesitant to embrace digital transformation. Overcoming this resistance and fostering a culture of acceptance and adaptability within the legal community is a long-term challenge. Achieving standardization in electronic evidence practices and ensuring the interoperability of various digital formats and systems is a complex task. Without consistent standards and protocols, the exchange and verification of electronic evidence may become cumbersome and error-prone. Implementing reforms in the justice system requires financial and human resources. Budgetary constraints and competing priorities may limit the ability of the government to invest in the necessary technology, training, and infrastructure required for electronic evidence practices. In an era of globalization, cross-border legal cases involving electronic evidence are becoming more common. Coordinating and collaborating with international counterparts on electronic evidence issues can be challenging due to differences in legal systems and standards. Addressing these challenges and hurdles demands a coordinated effort from government institutions, legal professionals, technology experts, and civil society. Overcoming these obstacles is essential to realizing the full potential of electronic evidence in Indonesia's justice system and ensuring that it remains a reliable and effective tool for the pursuit of justice. The Indonesian justice system stands at a pivotal juncture where embracing electronic evidence can bring about substantial improvements. Recognizing the opportunities for enhancing electronic evidence practices is crucial for the effective integration of technology into legal proceedings. Below, we explore some of these opportunities and innovative approaches that can propel Indonesia towards a more efficient and reliable justice system. One of the most promising opportunities lies in the development and implementation of a rapid verification mechanism for electronic evidence. This mechanism, as introduced in the previous chapter, can significantly expedite the verification process while upholding the integrity of the evidence. By collaborating with technology experts and forensic specialists, Indonesia can create a platform that allows for the swift and secure validation of electronic evidence. This not only reduces the burden on the courts but also ensures that electronic evidence is presented and

evaluated in a timely manner. Blockchain technology offers a transparent and tamper-proof way of storing electronic evidence. Exploring the integration of blockchain into the Indonesian justice system can enhance the authenticity and integrity of electronic evidence. Blockchain's decentralized nature ensures that once evidence is recorded, it cannot be altered without leaving a trace. This can be particularly valuable for cases where data integrity is crucial, such as financial fraud or intellectual property disputes. To bolster the admissibility and reliability of electronic evidence, the Indonesian justice system should encourage expert testimonies from forensic analysts and technology specialists. These experts can provide insights into the authenticity of electronic evidence, the methods of data collection, and the validity of digital signatures. By involving qualified experts, the courts can make well-informed decisions regarding the acceptance and weight of electronic evidence. Developing standardized procedures and guidelines for handling electronic evidence is essential. Indonesia can learn from international best practices and adapt them to its unique legal context. Standardization can streamline the process of presenting electronic evidence, making it easier for legal practitioners, judges, and litigants to navigate the complexities of digital information. Collaboration with technology companies can yield valuable insights and resources for enhancing electronic evidence practices. Tech companies often have access to cutting-edge tools and expertise in data security and verification. Partnerships with these entities can lead to the development of innovative solutions tailored to Indonesia's legal requirements. Indonesia has a host of opportunities at its disposal to improve the admissibility and reliability of electronic evidence. By embracing these opportunities and implementing innovative approaches, the Indonesian justice system can adapt to the evolving technological landscape, ensuring that electronic evidence is a valuable asset rather than a potential challenge.

Conclusion

In conclusion, evaluating the validity of emails can be complex due to challenges related to authorship and unauthorized access. Witness testimonies, especially from victims and whistleblowers, play a crucial role in authenticating email communications. Authenticating website

content is essential, particularly when dealing with archived web pages. Courts often require witness testimony, especially from website owners or sponsors, to establish the accuracy of digital evidence. The use of Internet archives can aid in this process. Validity assessment of text messages and social media posts relies on screenshots and witness testimonies. The potential for edited content underscores the importance of verifying the accuracy of digital messages. Distinguishing between digitally "edited" and "enhanced" photos is crucial in assessing their validity. Witness testimonies confirming the accuracy of photos are essential, and expert testimony may be required for digitally enhanced images. Differentiating between computer animation and simulation is important when assessing their accuracy. Courts need to consider the validity of simulations based on scientific principles.

Recommendations: Provide training and education to legal professionals, judges, and lawyers in Indonesia on the authentication of digital evidence. This should include understanding the challenges and methods of validating digital content. Develop standardized procedures for the admission and authentication of digital evidence in Court. These procedures should include guidelines for assessing emails, website content, text messages, and digital photographs. Encourage the availability of expert witnesses in digital forensics and digital photography to assist the courts in evaluating complex digital evidence. Expert testimony can enhance the reliability of conclusions. Establish digital forensics laboratories equipped with the latest technology to aid in the analysis and authentication of digital evidence. These labs can assist law enforcement agencies and the judiciary. Continuously update and adapt Indonesia's legal framework to address emerging challenges in the digital age. Ensure that laws regarding the admissibility and authentication of digital evidence are clear. Encourage collaboration between government agencies, law enforcement, legal professionals, and technology experts to develop best practices and guidelines for handling digital evidence. Raise awareness among the public about the importance of preserving digital evidence integrity and cooperating with law enforcement when needed. Align Indonesia's legal practices with international standards for digital evidence handling and authentication. Allocate resources to invest in technology and training for law enforcement and legal professionals to keep up with advancements in digital evidence. Regularly review the effectiveness of these

recommendations and gather feedback from legal practitioners to refine and improve digital evidence-handling practices. These recommendations aim to enhance the validity assessment of digital evidence in Indonesia's legal system and promote the fair and just use of such evidence in court proceedings.

Acknowledgments

The author acknowledges the National Librarian's invaluable assistance with the references in this article.

Bibliography

Bergman, Kristin. "Cyborgs in the courtroom: The use of Google Glass recordings in litigation." *Richmond Journal of Law & Technology* 20, no. 3 (2014): 11.

Bungert, Maximilian. "Do It for the Snap: Different Methods of Authenticating Snapchat Evidence for Criminal Prosecutions." U. Ill. *JL Tech. & Pol'y* (2021): 121.

Dyrda, Adam, and Maciej Próchnicki. "Expert's (Meta) Testimony: An Epistemological Perspective." In *Theory of Legal Evidence-Evidence in Legal Theory*, pp. 169-188. Cham: Springer International Publishing, 2022.

Flanagan, Elizabeth A. "# Guilty: Sublet v. State and the Authentication of Social Media Evidence in Criminal Proceedings." *Vill. L. Rev.* 61 (2016): 287.

Frieden, Jonathan D., and Leigh M. Murray. "The admissibility of electronic evidence under the federal rules of evidence." Richmond *Journal of Law & Technology* 17, no. 2 (2011): 5.

Hlavka, Heather R., and Sameena Mulla. "That's How She Talks": Animating Text Message Evidence in the Sexual Assault Trial." *Law & Society Review* 52, no. 2 (2018): 401-435.

Hong, Ilyoung. "International Digital Forensic Investigation at the ICC." *Handling and Exchanging Electronic Evidence Across Europe* (2018): 125-139.

Kaneko, Hironao. "Electronic Evidence in Civil Procedure in Japan." Digital Evidence & Elec. *Signature L. Rev.* 5 (2008): 211.

Novak, Martin. "Digital evidence in criminal cases before the US courts of appeal: Trends and issues for consideration." *Journal of Digital Forensics, Security and Law* 14, no. 4 (2020): 3.

Rijavec, Vesna, and Tomaž Keresteš, eds. *Dimensions of evidence in European civil procedure*. Kluwer Law International BV, 2015.

Tran, Quynh Anh. "Basic Issues of Evidence and Electronic Evidence in Civil and Commercial Dispute Resolution." In *Electronic Evidence in Civil and Commercial Dispute Resolution: A Comparative Perspective of UNCITRAL*, the European Union, Germany, and Vietnam, pp. 51-87. Cham: Springer Nature Switzerland, 2022.

Tran, Quynh Anh. "The Authentication of Electronic Evidence." In *Electronic Evidence in Civil and Commercial Dispute Resolution: A Comparative Perspective of UNCITRAL*, the European Union, Germany and Vietnam, pp. 167-210. Cham: Springer Nature Switzerland, 2022.

Tran, Quynh Anh. "The Admission of Electronic Evidence in Civil and Arbitral Proceedings." In *Electronic Evidence in Civil and Commercial Dispute Resolution: A Comparative Perspective* of UNCITRAL, the European Union, Germany and Vietnam, pp. 211-231. Cham: Springer Nature Switzerland, 2022.

Tran, Quynh Anh. "The Significant Types of Electronic Evidence." In *Electronic Evidence in Civil and Commercial Dispute Resolution: A Comparative Perspective* of UNCITRAL, the European Union, Germany and Vietnam, pp. 89-113. Cham: Springer Nature Switzerland, 2022.

Zander, Michael. *The police and criminal evidence Act 1984*. Sweet & Maxwell, 2013.