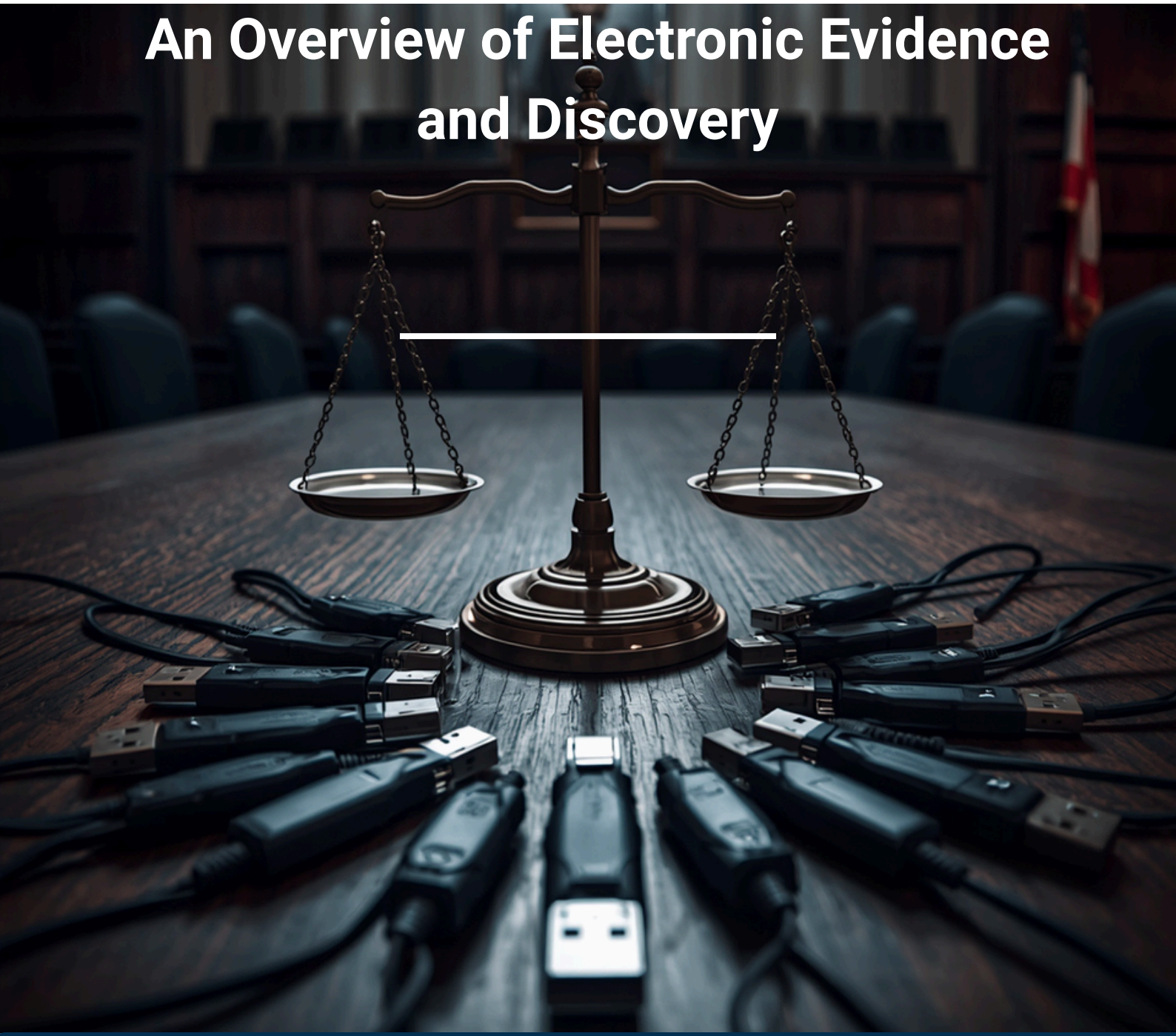
DIAMOND ADVOCATES

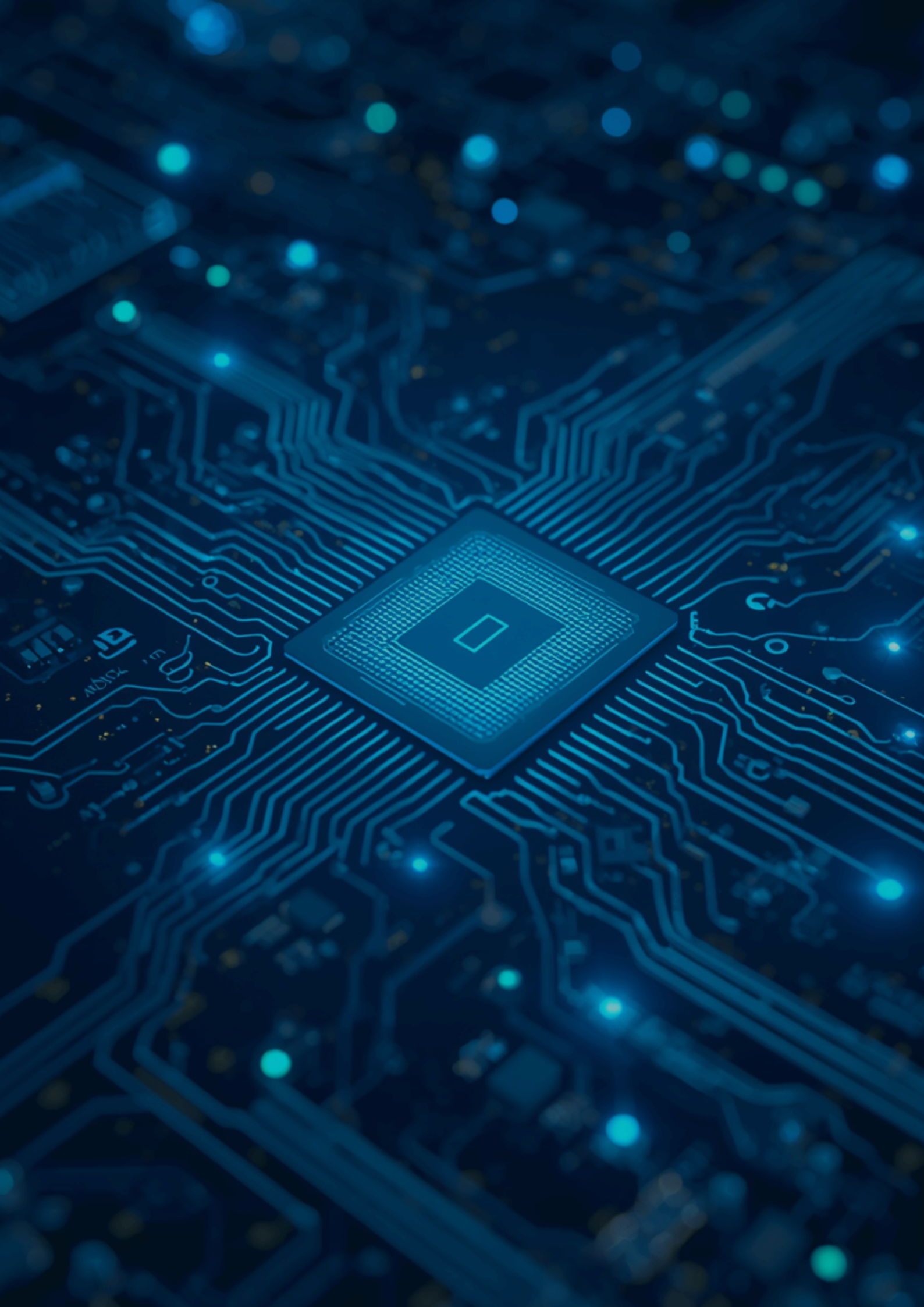
EXCLUSIVE REGIONAL PARTNER
WONE GLOBAL
wone

E-DISCOVERY IN LITIGATION

An Overview of Electronic Evidence and Discovery



Diamond Brief Series- Vol.1 Issue 5



Introduction

Developments in digital technologies over the past few decades have profoundly affected every area of law, from the practice of individual lawyers to court procedures. The traditionally conservative legal profession is now compelled to embrace these changes to stay relevant in the changing world.

Discovery is a crucial part of court procedure in common law jurisdictions. It allows each party to obtain the information needed to prepare for trial, evaluate the strengths and weaknesses of their case, and develop strategies for success. As more information is stored electronically, the need for an electronic form of this litigation phase has emerged.

Electronic discovery(e-Discovery), refers to the process of identifying, collecting, and producing electronically stored information (ESI) in response to a request for production in a lawsuit or investigation.

The traditionally conservative legal profession is undergoing tremendous changes with the introduction of new technologies. Over the years, technology has quickly displaced outdated processes. However, the real acceleration of the digital transformation in the legal profession happened with the COVID-19 pandemic in 2020.

What is Electronically Stored Information (ESI)?

Electronically Stored Information refers to any data that is created, manipulated, stored, and best utilized in a digital format. ESI encompasses a wide range of digital data, including emails, online documents, spreadsheets, databases, digital images, presentations, audio and video files, social media posts, websites, cloud storage files, mobile device data, chat and instant messaging logs, backups and archives, social media content and deleted or encrypted files that require forensic recovery amongst others.

ESI is dynamic and often contains metadata such as time-date stamps and author information. This complexity, along with the volume of data, necessitates the use of advanced technology to handle e-Discovery effectively.

Admissibility of Digital/ Electronic evidence

Electronic evidence is information created or stored in binary form that may be relied on in court to prove or disprove an assertion.

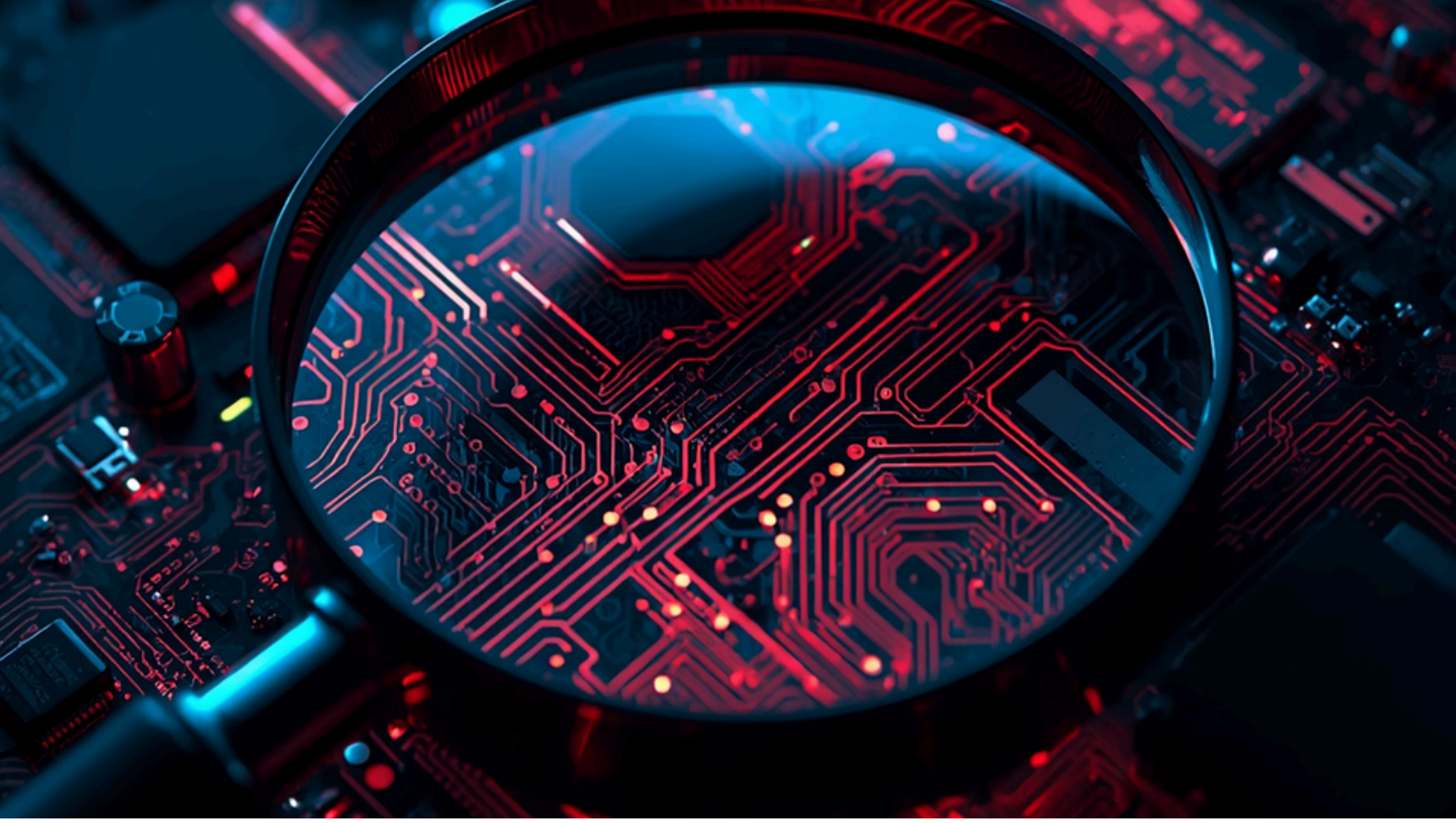
There are basically two types of electronic evidence i.e., data stored on computer systems and information transmitted electronically through communication networks.

On the other hand, digital evidence admissibility refers to the set of legal and technical conditions that a digital file must satisfy before a court can accept it as proof. A file is admissible when it establishes a fact relevant to the case, remains unaltered during forensic processing, and produces results that are valid, reliable, and reproducible. This means that there is a need to capture origin data (device identifiers, GPS coordinates, timestamps), seal the file cryptographically at the moment of creation, and maintain an auditable chain of custody from capture to courtroom. Without these layers, courts treat digital files as inherently unreliable, because metadata can be edited, timestamps can be spoofed, and file contents can be altered without leaving visible traces.

Digital evidence is only admissible in court when it meets four conditions: authenticated origin linking the file to a verified source and timestamp, proven integrity confirming no alteration occurred after capture, a documented chain of custody recording every access event, and compliance with applicable legal frameworks. This is to ensure authenticity of the digital evidence being presented in court due to factors like velocity, volatility and fragility of electronic data.

Additionally, the present law on evidence in Uganda recognizes the 'Best Evidence Rule' requires that only original documents in a written form can be admissible in courts of law- Section 60-64 of the Evidence Act Cap 6. However, due to technological advancement, more laws were enacted in Uganda to fill the technology legal gap for example the Electronic Transactions Act 2011 under which the Best Evidence Rule is extended. Section 8(1) (a) and (b) of this Act which is to the effect that the best evidence rule is fulfilled upon proof of the authenticity of the electronic records system in or by which the data was recorded or stored.

NB: Key to eDiscovery is the preservation of original content and metadata to avoid claims of spoliation or tampering with evidence.



Reliability of Electronic Evidence

Electronic evidence can be relied on if the party who alleges has established its authenticity and the opposite party has not produced any proof of tampering. Therefore, courts consider the following factors in assessing the reliability of electronic evidence as stated in the case of **Amongin Jane Frances Akili v Lucy Akello & Anor (HCT-02-CV-EP-0001-2014):**

1. The reliability of the equipment used.
2. The manner in which the basic data was initially entered.
3. The measures taken to ensure the accuracy of data as entered.
4. The method of storing the data and precautions taken to prevent loss or alteration.
5. The reliability of the computer programs used to process the data.
6. The measures taken to verify the accuracy of the program.
7. What software was used to preserve digital evidence in its original form and to authenticate it for admissibility.
8. The competence of the person who accessed the original data.
9. This person must be competent to do so and able to give evidence explaining the relevance and implication of what he did.
10. An independent third party should be able to examine the process and achieve the same results.

The e-Discovery Process

Electronic discovery refers to the legal process of identifying, preserving, collecting, processing, reviewing, and producing electronically stored information for use in civil litigation, criminal investigations, and regulatory compliance matters. Worldwide, e-Discovery has become indispensable as digital communications and cloud storage replace paper records across commercial and personal spheres.

The Electronic Discovery Reference Model (EDRM) defines seven stages in e-Discovery to ensure defensible, efficient evidence handling i.e.,

1. Identification: Locate potentially relevant electronically stored information across all custodian devices, servers, cloud accounts, and backup systems.
2. Preservation: Implement legal holds to prevent deletion or alteration of identified data, ensuring evidence remains intact.
3. Collection: Extract preserved data using forensically sound methods that maintain metadata and verify file integrity.
4. Processing: Convert collected data into reviewable formats, remove duplicates, and apply initial filtering to reduce volume.
5. Review: Legal teams examine processed documents for relevance, privilege, and confidentiality before disclosure.
6. Analysis: Identify patterns, relationships, and key evidence through advanced search, concept clustering, and timeline analysis.
7. Production: Deliver responsive documents to opposing parties or regulators in agreed formats meeting court requirements.

Data Protection in e-discovery

The General Data Protection Regulation (GDPR) governs how personal data within digital evidence is collected, processed, stored, and accessed. Any evidence that includes personally identifiable information (faces in photos, names in documents, location data) must comply with GDPR principles: lawfulness, purpose limitation, data minimization, and security. This is equally provided for in the Data Protection and Privacy Act 2019 under Section 3 which mandates collection of adequate personal data, relevant and limited to what is strictly necessary for the purposes it was processed and retained for the authorized period of time. Failure to comply leads to fining of the non-compliant party.

Notwithstanding the foregoing framework, critics have raised concerns that e-Discovery, as currently practiced, may disproportionately burden smaller litigants who lack the financial resources or technical infrastructure to engage in sophisticated electronic evidence management. The costs associated with forensic collection, processing, and review of ESI can be prohibitive, creating an asymmetry that may disadvantage individuals and small entities against well-resourced corporations or government bodies.

This concern, while legitimate, does not undermine the necessity of e-Discovery; rather, it calls for proportionality in its application. Courts and legislators have increasingly recognized this tension. Rules governing discovery in many jurisdictions now incorporate proportionality principles, requiring that the scope of e-Discovery be calibrated to the complexity and stakes of the litigation.

In Uganda, the Civil Procedure Rules grant courts broad discretionary powers to manage and limit the scope of discovery where it would be unduly onerous, and these powers equally extend to electronically stored information.

Furthermore, concerns around privacy and data protection, particularly in the context of the Data Protection and Privacy Act 2019, must be balanced against the legitimate interests of justice. While data minimization and purpose limitation are important principles, the evidentiary imperatives of litigation may, in appropriate circumstances, justify the processing of personal data beyond its originally intended purpose. This is a recognised exception under data protection law, provided there exists a lawful basis and adequate safeguards are in place.

The courts, as neutral arbiters, are well placed to strike this balance on a case-by-case basis.

Conclusion

Electronic discovery has fundamentally transformed the landscape of modern litigation. As the volume of digitally generated information continues to grow exponentially, the ability to identify, preserve, collect, and produce Electronically Stored Information in a legally defensible manner has become an indispensable competency for legal practitioners, judges, and litigants alike.

The Ugandan legal framework, anchored by the Electronic Transactions Act 2011 and the Data Protection and Privacy Act 2019, provides a foundational basis for the admissibility and management of electronic evidence. However, the rapid pace of technological change demands continued legislative attention and judicial adaptability. Courts must be equipped not only with updated rules of procedure, but also with the technical understanding necessary to adjudicate e-Discovery disputes fairly and efficiently.

-END-

THE AUTHOR

Vera Kabasiita Nakatumba
Legal Associate, Corporate and Commercial Department

DIAMOND ADVOCATES | Partner wone GLOBAL

Contact us:

Plot 1 Lourdel Road
Lourdel Towers, 5th Floor
P.O BOX 133174 Kampala-Uganda
Tel: +256 414 671 838
www.diamondadvocates.com