# ADVOCATING CHAIN OF CUSTODY AND GOVERNANCE OF DIGITAL EVIDENCE IN NEPAL

HUMAN RIGHTS AND JUSTICE CENTRE

CYRILLA
Advancing Access to Digital Rights Law

# POLICY PAPER

# ON

# ADVOCATING CHAIN OF CUSTODY AND GOVERNANCE OF DIGITAL EVIDENCE IN NEPAL

HUMAN RIGHTS AND JUSTICE CENTRE

2024

# Table of Contents

# 1. INTRODUCTION

## 1.1 Historical Perspective

Digital evidence has emerged as a crucial component in the investigation and prosecution of various criminal activities. Crimes previously conducted through traditional mediums, such as physical documents or verbal communication, are now being perpetrated using digital devices. For instance, defamation, once accomplished through spoken word or printed materials, now often occurs through social media platforms and electronic communication. Similarly, corruption, previously involving alteration of physical records, has evolved into manipulation of data within digital databases. Moreover, the misappropriation of funds within banking institutions, once carried out through manual alteration of records in physical files and other tangible mediums, has now transitioned to electronic means. With the shift in methods and the prevalence of electronic devices in criminal activities, evidence trails primarily exist in digital formats, underscoring the need for effective governance of digital evidence.

With the pivotal role of digital evidence in the criminal investigation process, concerns have arisen regarding its admissibility, credibility, and reliability. Fundamental to evidence law is the requirement to present the best evidence in court. This entails providing evidence that is not only admissible but also credible and trustworthy, without raising doubts regarding the accused or the allegations against them. Technological advancements have facilitated the utilization of diverse digital techniques in presenting evidence to courts. Digital evidence has been utilized across various domains, including log analysis, database, log trials, audio enhancement, photograph enhancement, forensic video analysis, and the digital enhancement of latent fingerprints.

The legal value of digital evidence in court is significant and continues to grow with the increasing reliance on digital technologies in everyday life. Digital evidence encompasses various forms of electronic data, including emails, text messages, social media posts, photos, videos, computer files, and electronic transactions. The admissibility and weight given to digital evidence in court depend on several factors, including its relevance, authenticity, reliability, and compliance with legal standards and procedures. When properly collected, preserved, and presented, digital evidence can be highly persuasive and influential in proving or disproving facts in dispute.

Courts increasingly recognize the importance of digital evidence in modern litigation and criminal proceedings, often relying on it to establish timelines, corroborate witness testimony, demonstrate

intent or motive, and connect individuals to criminal activities. However, challenges such as data privacy concerns, issues of authenticity, and the need for specialized expertise in digital forensics can impact the admissibility and reliability of digital evidence. Therefore, it's crucial for parties presenting digital evidence to adhere to legal standards and procedures, including demonstrating the authenticity and integrity of the evidence, maintaining chain of custody records, and providing expert testimony when necessary. Forgery/tampering of physical documents used to be a way of misleading a judicial process, but the recent technological advancements have extended the definition of forgery/ tampering, whereby challenging the credibility of evidences which are relied upon while dispensing justice. Overall, digital evidence holds considerable legal value in court proceedings and is expected to play an increasingly prominent role in the justice system as technology continues to evolve.

The use of electronic evidence in criminal proceedings, including photographs, videos, and audio recordings, has been a longstanding practice. Since the Nuremberg trials, these materials have played a crucial role in documenting and prosecuting various types of crimes. In recent decades, with the increase in technology for the criminal activities the use of technology for committing crimes has increased which has been witnessed in domestic, regional and international court cases. Apart from this, digital technologies are also serving a tool to record evidences related to crimes. In both of the scenarios, the recognition of digital records as evidences for the purpose of deciding any case has become the need of the time. For example, over 4 million videos related to the Syrian conflict have been uploaded on YouTube alone, surpassing the duration of the conflict itself. International Criminal Court ( ICC) investigators and prosecutors have adapted to evidence collection trend by collecting user-generated digital and open-source evidence for use in trials. The Office of the Prosecutor began collecting digital evidence in 2008 in the Bemba case[1], and video evidence was introduced in the first trial before the Court, Prosecutor v Thomas Lubanga Dyilo[2]. By 2011, this type of evidence had been collected in investigations related to Kenya, Ivory Coast, and Libya. To ensure the authenticity,

[1] The Prosecutor v. Jean-Pierre Bemba Gombo, Case No. ICC-01/05-01/08, Judgment Pursuant to Article 74 of the Statute, Int'l Crim. Ct. (Mar. 21, 2016), available at: https://www.icc-cpi.int/sites/default/files/CaseInformationSheets/BembaEng.pdf

[2] Prosecutor v. Thomas Lubanga Dyilo, Case No. ICC-01/04-01/06, Judgment Pursuant to Article 74 of the Statute, Int'l Crim. Ct. (Mar. 14, 2012), available at : https://www.icc-cpi.int/sites/default/files/CaseInformationSheets/LubangaEng.pdf

accuracy, confidentiality, and preservation of court proceedings, the Court has developed an 'e-Court Protocol'.[3]

## 1.2 An Overview of Evidence Collection Procedures and Practices in Nepal

The collection of digital evidence relies on a set of fundamental principles to maintain its integrity, authenticity, and admissibility in legal proceedings. Firstly, integrity is paramount, requiring that digital evidence remains unaltered throughout the collection and analysis process. Secondly, establishing a clear chain of custody is essential, documenting the handling of evidence from collection to presentation in court to prevent tampering.

Authenticity is another crucial aspect, necessitating verification of the evidence's origin and ensuring it hasn't been fabricated or altered. It also denotes the genuineness of something, confirming its true identity and integrity. Specifically concerning documentary materials, authenticity signifies that an entity must preserve both its identity and integrity, remaining unaltered or tampered with from its creation until its utilization as a source of information or submission as evidence.[4]

Furthermore, digital evidence must be relevant to the case and meet legal standards for admissibility, including reliability and procedural compliance. Privacy and legal compliance are also paramount, requiring adherence to relevant laws and regulations governing data collection and handling. By upholding these principles, digital evidence collection maintains the integrity of legal proceedings while safeguarding the rights and privacy of all parties involved.[5]

In Nepal, the procedures and protocols for gathering evidence in criminal cases are outlined by the Criminal Procedure Code, 2074 (2017). These guidelines govern the collection, handling, and presentation of evidence by law enforcement authorities. At the initial stage, evidence collection begins at the crime scene, where physical evidence such as fingerprints, Deoxyribonucleic acid (DNA) samples, and weapons are gathered. Witness statements are also recorded to capture pertinent

---

3 Mark Kersten, Challenges and Opportunities: Audio-Visual Evidence in International Criminal Proceedings Posted on March 4, 2020, cited on https://justiceinconflict.org/2020/03/04/challenges-and-opportunities-audio-visual-evidence-in-international-criminal-proceedings/

4 Duranti, Luciana, and Allison Stanfield. "Authenticating Electronic Evidence." *Electronic Evidence and Electronic Signatures*, edited by Stephen Mason and Daniel Seng, CMB-Combined volume, 5, University of London Press, 2021, pp. 236–78. *JSTOR*, http://www.jstor.org/stable/j.ctv1vbd28p.13. Accessed 27 Mar. 2024.

5 Digital Evidence and the New Criminal Procedure Author(s): Orin S. Kerr Source: Columbia Law Review , Jan., 2005, Vol. 105, No. 1 (Jan., 2005), pp. 279-318 Published by: Columbia Law Review Association, Inc. Stable URL: https://www.jstor.org/stable/4099310

information related to the crime. Additionally, forensic experts may analyze physical evidence for further insight. With the rise in technological advancements, electronic evidence, such as data from computers and mobile phones, is increasingly prominent and subject to specialized forensic examination.

For digital evidence to be admissible in court, it must be collected effectively, maintained with a proper chain of custody by the investigating authority, and transferred to the court under secure and established procedures. This ensures the evidence's integrity and credibility are preserved throughout the process.

It is imperative to maintain the chain of custody of collected evidence to ensure its integrity and admissibility in court. All evidence collection processes must adhere to legal standards and protocols to safeguard the rights of the accused. In cases involving transnational crimes, Nepal may seek international cooperation through diplomatic channels or mutual legal assistance treaties. Admissibility of evidence from other countries hinges on its legality, compliance with international agreements, and relevance to the case. Overall, the procedures of evidence collection in Nepal are designed to uphold justice while respecting the rights of all parties involved.

## 1.3 Importance of Chain of Custody and Governance of Digital Evidence

The concept of continuity of custody, also known as the chain of evidence, is crucial to consider, particularly concerning electronic evidence. Electronic evidence is susceptible to alteration, necessitating a demonstration of its integrity and ensuring it hasn't been tampered with since its acquisition or copying. It's essential to meticulously document the custody of electronic evidence, especially in cases involving multiple hardware items and computers, to establish a clear link between the hardware and the copied evidence. This documentation should include details such as who collected the evidence, how and where it was collected, who took possession of it, storage procedures, protections while in storage, and records of anyone accessing the evidence and reasons for doing so. Given the prevalence of online storage and services, managing access and custody of records before they become evidence is also important, especially when cryptographic safeguards are impractical.[6] In context of Nepal, cryptographic safeguards become impractical due to lack of technical resources and complexity of related tools, there are inoperability issues when technologies become incompatible and

[6] Wilson, Nigel, et al. "Proof: The Technical Collection and Examination of Electronic Evidence." *Electronic Evidence and Electronic Signatures*, edited by Stephen Mason and Daniel Seng, CMB-Combined volume, 5, University of London Press, 2021, pp. 429–87. *JSTOR*, http://www.jstor.org/stable/j.ctv1vbd28p.16. Accessed 27 Mar. 2024.

there is lack of standardization, human errors can also render risks of loss or inaccessibility of data, similarly there will be legal and procedural challenges supplemented by increased costs of implementation. Therefore, it is crucial to maintain a proper chain of custody with adequate safeguards to protect privacy of individual data and ensuring credibility of evidences.

## 2. GUIDELINE FOR HANDLING DIGITAL EVIDENCE: INTERNATIONAL PERSPECTIVE

With the development of information technology, various standards have developed in international platform for identification, collection, acquisition and preservation of digital evidence. Notably, the ISO/IEC 27037:2012[7] which provides guidance to individuals with respect to common situations encountered throughout the digital evidence handling process and assists organization in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions; the ISO/IEC 27042[8] Guidelines for analysing digital evidence; INTERPOL's Operational guidelines on digital forensic practices; Europol's European Cybercrime Centre (EC3) Frameworks and Toolkits for handling digital evidence; UNODC's Cybercrime Repository which contains resources and manuals for handling electronic evidence in criminal investigations; Budapest Convention on Cybercrime[9] which provides provisions particularly in cross-border investigations and ensuring preservation and authenticity of digital evidence; the International Association of Computer Investigative Specialists (IACIS) also has put forward certifications and best practices for digital forensics professionals. The Association of Chief Police Officers (ACPO) guidelines for digital evidence also outlines best practices for proper handling, collecting, preservation, and analysis of electronic data in criminal investigations. It emphasizes maintaining the integrity of digital evidence, ensuring it is not altered during acquisition or examination. The guidelines advocate for proper documentation of all actions taken, adherence to legal protocols, and secure storage to prevent

[7] ISO/IEC JTC 1/SC 27, *Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence*, ISO (2012), available at, https://webstore.ansi.org/preview-pages/INCITS/preview_INCITS+ISO+IEC+27037+2012+(R2019).pdf?srsltid=AfmBOoqREc1Pliql6CQCOGXgN4J0S3mPjdSRt9Ib_XYJjPLL1Yf8zWG_

[8] ISO/IEC 27042: ISO/IEC JTC 1/SC 27, *Information Technology—Security Techniques—Guidelines for the Analysis and Interpretation of Digital Evidence*, ISO (Year varies)

[9] Council of Europe, *Convention on Cybercrime* (ETS No. 185), opened for signature Nov. 23, 2001

tampering of evidences. The goal of these instruments is to ensure digital evidence remains admissible in court and supports effective and fair investigations.

Considering the above international standards, we can observe that preceding the investigation and examination of electronic evidence, there's a method called 'forensic triage' gaining attention in forensic and law enforcement circles. It encompasses various processes, tools, and methodologies aimed at prioritizing digital forensic investigations more effectively. However, it's important to note that forensic triage isn't suitable for every case and should be used alongside proper risk assessment by trained individuals.

When employing digital triage techniques, it is important to balance rapid identification of material of interest with the risk of stopping further analysis, potentially missing exculpatory or more significant material. For example, in a case involving the downloading of indecent images and child abuse, keyword and hash set analysis can quickly identify known indecent images. However, relying solely on triage results may lead to overlooking more serious offenses. Therefore, digital triage should be seen as an early investigation technique aiding informed decisions rather than the sole investigative method.

## 2.1 Handling Electronic Devices

Digital evidence professionals are advised to uphold high standards in collecting and handling digital evidence, regardless of whether they're involved in criminal or civil cases. Improper handling of digital data can lead to challenges regarding the destruction of data and the employment of inadequate practices[10].

Following Association of Chief Police Officers Guidelines (ACPO guidelines)[11] is crucial to ensure proper handling of electronic evidence, considering its volatile and easily alterable nature. The principles stress the importance of preserving data integrity, competence in accessing original data,

---

10 *Stanford International Bank Limited (in liquidation) v. Hamilton-Smith,* High Court (Antigua), See : https://ag.vlex.com/vid/alexander-m-fundora-applicant-805812073

11 Williams, Janet. "Acpo good practice guide for digital evidence." *Metropolitan Police Service, Association of chief police officers, GB* (2012): 1556-6013., *Good Practice Guides for Digital Evidence (the latest of five revisions coming in 2012, the first being in 1998 [2]) are considered to provide core information for practitioners operating in the digital forensics field in England and Wales.* The,Principle 1, No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court. Principle 2, In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions. Principle 3, An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result, Principle 4: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

maintaining an audit trail, and overall responsibility for adherence to legal standards and principles in digital evidence handling. Despite the importance placed by digital evidence professionals on adhering to guidelines for maintaining the authenticity and integrity of digital data, courts may sometimes overlook these considerations. The failure to understand the significance of digital forensics in data seizure may undermine the integrity of legal proceedings. Implementing best practices, such as generating hash values upon forensic imaging of seized hard drives, could help ensure the integrity of digital evidence, but such practices may not always be fully appreciated or utilized by courts or defense teams.

## 2.2 Identifying Electronic Evidence

The discovery of evidence in digital form can often be the initial indication of wrongdoing, prompting the need for investigation. Initiating an investigation can inadvertently alter electronic evidence. Having appropriate procedures in place to initiate and conduct investigations is essential. In both civil and criminal cases, there are obligations to disclose relevant documents, and investigating authorities are expected to adhere to recognized guidelines. ACPO Good Practice Guide for Digital Evidence outlines four main phases for handling evidence: collection, examination, analysis, and reporting, which may be augmented with an initial assessment phase in light of forensic triage techniques.

## 2.3 Gathering of Electronic Evidence

Once the need to gather digital evidence is determined, specific procedures should be followed to guide digital evidence professionals in handling the scene and identifying and seizing evidence if required. It is now standard practice to document the scene through photography or video recording, including capturing the layout of hardware. The investigator must then assess which physical evidence, such as computers or storage devices, should be retained, with reference to established guidelines. It's crucial to prevent tampering with hardware or networks and to ensure that only properly trained personnel handle computers designated for seizure.

One significant challenge with digital evidence is its susceptibility to alteration or destruction. Digital devices, being volatile, can lose crucial data when powered off. Arresting suspects who are physically present at a computer requires special care, as they may attempt to delete or disrupt incriminating files.

## 2.4 Copying Electronic Evidence

Copying electronic evidence involves adhering to several key principles outlined in the ACPO Guide. These include: Avoiding any actions that may alter data relied upon in court, ensuring that those

accessing original data are competent and can explain their actions, creating and preserving an audit trail of all processes applied to digital evidence and ensuring that the person in charge of the investigation upholds the Evidence law and these principles. When dealing with networked systems, it's essential to understand the topology and sources of digital evidence across various locations. The process of copying electronic evidence should aim to produce an exact replica without altering the original data. Hashing processes are used to verify the authenticity of copied files.

Maintaining the quality of copied digital files is crucial, as highlighted in legal cases like *The Gates Rubber Company v Bando Chemical Industries Limited*[12], where the mishandling of evidence led to its loss of probative value in court. Digital evidence professionals must sometimes make decisions based on principles of good practice, especially in unique situations like live banking systems. Examining the surrounding area of the scene can also yield relevant materials for disclosure or criminal investigations, complementing the digital evidence gathered. This example illustrates that a loss of evidence dependability can lead to significant challenges for the concerned party, which may not always be adequately addressed in every situation.

## 2.5 Preserving Electronic Evidence

Electronic evidence must undergo validation to ensure its probative value. Digital evidence professionals routinely copy data from various disks or storage devices, necessitating measures to prove the integrity of the duplicated evidence. Electronic fingerprinting, a cryptographic technique, associates a unique identifier with each file or storage device, enabling verification of data integrity at the time of collection.

The continuity of custody is crucial in preserving electronic evidence, requiring meticulous documentation of its collection, storage, and handling to demonstrate integrity and prevent tampering. When transporting and storing hardware and digital evidences, precautions must be taken to protect against damage or data corruption, which may be caused by factors like temperature, humidity, and magnetic effects.

The emergence of cloud computing presents complex challenges for digital forensics, as evidence stored in the cloud is distributed across multiple servers and managed automatically. Retrieving such evidence may require cooperation from service providers, raising jurisdictional issues. Forensic triage

12 United States Court of Appeals, Tenth Circuit, 9 F.3d 823 (10th Cir. 1993)

becomes essential for timely evaluation and preservation of online data, particularly in cases where remote deletion is a risk.

## 2.6 Analysis of Electronic Evidence

While analysing various aspects of digital evidence, we have to acknowledge the critical role of digital evidence professionals in both obtaining and analyzing electronic evidence. Merely obtaining evidence is not sufficient; it must be thoroughly analyzed to ensure its accuracy and reliability. Failure to assess digital evidence properly can lead to false assumptions.

In *Liser v Smith*[13], the investigators relied solely on a single, unverified statement from the bank manager regarding the discrepancy in the surveillance tape's timing. Despite having ample time for investigation, they failed to verify the accuracy of the tape's time stamp, leading to a wrongful arrest. This case underscores the importance of verifying electronic evidence thoroughly, especially in deliberate, slowly unfolding investigations. Similarly, in *Mogford v Secretary of State for Education and Skills*[14], inconsistencies in the suspect's testimony and the timing of file system activities were crucial in establishing guilt. The failure to corroborate the suspect's story and the timing of computer activity played significant roles in the tribunal's decision.

Overall, the excerpt stresses the importance of meticulous analysis and verification of electronic evidence to ensure its accuracy and reliability in legal proceedings. Simply relying on digital data without proper scrutiny can lead to erroneous conclusions and unjust outcomes.[15]

---

13 Jason Liser Plaintiff v. Jeffrey Smith et al, United States District Court, D. Columbia, No. CIV.A.00-2325 (ESH) (D.D.C. Mar. 26, 2003)

14 England and Wales care Standards Tribunal, Mogford v Secretary of State for Education and Skills [2002] EWCST 11(PC) (26 June 2002), https://www.bailii.org/ew/cases/EWCST/2002/11(PC).html

15 Mason, Stephen, et al. "Proof: The Technical Collection and Examination of Electronic Evidence." *Electronic Evidence*, edited by Stephen Mason and Daniel Seng, 4th ed., University of London Press, 2017, pp. 285–338. *JSTOR*, http://www.jstor.org/stable/j.ctv512x65.16. Accessed 27 Mar. 2024.

# 3. LEGAL FRAMEWORK AND JUDICIAL DECISIONS ON ADMISSIBILITY OF DIGITAL EVIDENCE IN NEPAL

## 3.1 Major National Laws

### i. Criminal Procedural Code of Nepal 2074 (2017)

Provisions relating to civil and criminal evidences within the Civil and Criminal Codes of Nepal may be invoked to address various aspects of digital evidence, including issues related to privacy, data protection, cybercrimes, and the admissibility of electronic records. Criminal Procedure Code, 2017 and Regulation Related to Investigation of Offence, 2017 governs the procedure for criminal investigations and trials in Nepal. While it does not specifically address digital evidence, its provisions on evidence collection, examination, and presentation apply to digital evidence. The prevailing legal standards outline the standards and procedures for the admissibility of evidence in court, which indirectly includes digital devices, however refrains the inclusion of digital evidences inside those devices. The contents of any device fall under the premise of Privacy laws, and proper reference to the Privacy laws are not observed in the provisions of the Criminal Procedural Code.

In Nepal, the codes acknowledge electronic records as admissible evidence within the judicial system. The digital records and evidence are categorized and treated as part of document evidence. There are no specific provisions related to the collection of data because digital records are not regarded as separate forms of evidence. Instead, they fall under the umbrella of documents on evidence within the legal framework.

The Criminal Procedure delineates procedures for evidence handling, from collection to presentation in court. Section 6 of the Criminal Procedure Code mandates prompt police action upon receiving information, including preventing evidence tampering and offender escape. Police must seize evidence, arrest offenders, and document findings, with provisions for requesting external assistance if immediate seizure is impractical. This ensures evidence integrity and offender apprehension. Similarly, Section 8[16] of the Criminal Procedure Code specifies procedures for investigating reported offenses, including evidence collection. When submitting a case for prosecution, the investigating

[16] Section 8 of Criminal Procedure code

authority retains custody of evidence and the accused, presenting them in court as directed by the government attorney. [17]

**ii. Electronic Transaction Act 2063 (2008)**

In the legislation of Nepal, the term "electronic evidence" is not defined. However, the Electronic Transaction Act 2063 (2008) provides definitions for "electronic record" which includes the data, record, image or sound transmitted, received or stored in an electronic form by generating the same through any means (Section 2 (v)) and "electronic form" means a form of information transmitted, received or stored by generating the same through the means of magnetic, optical, computer memory or similar other devices.

Section 4 of Electronic Transaction Act recognises legal value to the electronic records, establishing that where the prevailing law requires any information, documents, records or any other matters to be kept in written or printed typewritten form, then, if such information, document, record or the matter is maintained in an electronic form by fulfilling the procedures as stipulated in this Act or the Rules made hereunder, such electronic record shall also have legal validity.[18]

**iii. The Privacy Act 2075 (2018)**

Section 19 of The Privacy Act outlines regulations concerning the privacy of electronic communications. It asserts that individuals have the right to maintain the privacy of their personal information, documents, correspondence, data, and characters stored electronically. Unauthorized access to or violation of this privacy is prohibited. Without consent from the individual or lawful authorization, no one can intercept electronic communications or record conversations using mechanical devices. However, this provision does not apply to publicly made speeches or statements. Exceptions to these rules can be made with the consent of the individual or under the order of an authorized official. Further details regarding electronic notice and data privacy are provided as prescribed by law.

However, there is a lack of detailed laws concerning collection of digital evidence , and the decision making procedure. For instance: during any criminal investigation, the evidence related to an offence can be retained in accordance with established rules. However, other unrelated things are not supposed

17 Sec 38 of Criminal Procedure code

18 Section 4 of Electronic Transactions Act

to be taken into custody; by this analogy, personal data contained in the devices like laptop, mobile phones and other storage devices which are not related to the offence, remain vulnerable. It is imperative that the state implements proper mechanisms to protect such personal and private information. Current practices concerning the admissibility of evidence are inadequate, posing risk that Courts may rely on untrustworthy evidence or evidence obtained through unlawful means.

**iv. Evidence Act 2031 (1974)**

The Evidence Act of Nepal provides general provisions regarding the admissibility and evaluation of evidence in legal proceedings. Section 35, Chapter 6 is dedicated to documentary evidence, grounding the fundamental rules for admissibility.

The second Amendment in the Evidence Act of 2020 has made substantive amendments recognizing digital and electronic evidence. Upon amendment, section 2(c) of the Evidence Act has defined the digital or electronic version of a public document defined by prevailing laws as a public document. Furthermore, section 6 provides the things that are assumed by the court which include that the contract or document made by digital or electronic transaction is assumed by the court to be a valid agreement or deed and the transaction done by digital or electronic signature is also assumed to be valid. Section 13A (amended by the second amendment) provides that things that are electronically recorded in audio-visual medium are admissible as evidence. The section further provides that the court may record the audio visual recorded in digital form in the same form or have it scripted thereof. Furthermore, Section 14 of the Evidence Act provides that the details kept in digital and electronic mediums in the course of regular transactions or business is admissible as evidence in court. Section 35 of the Evidence Act provides that the information mentioned in any deed should be justified by submitting the deed thereof. The deed has been further clarified by the section stating that any subject matter recorded in a digital or electronic record and printed or stored in optical or electro-magnetic form or published or re-published is also regarded as the deed. Section 52 of the Evidence Act provides that in case the court needs to confirm the technicality of the issue, the court may call for such expert witness in the court as a witness of the court who is to be provided with an opportunity for cross-examination by the parties. Pursuant to this Act, the expert witnesses play a major role in digital evidence cases by providing their professional opinion and testimony, therefore expert witnesses should stay up-to-date about digital forensics research and literature works and be prepared to defend their methods, findings and conclusions before the court.

**v. National Cybersecurity Policy 2080 (2023)**

While not a law per se, Nepal has a national cybersecurity policy which outlines strategies for addressing cybersecurity challenges, including cybercrimes and the protection of digital information. This policy can guide on handling digital evidence related to cybercrimes.

## 3.2 Facilitating State Access to Digital Evidence Across Borders: Legal Frameworks and Mechanisms

Nepal's legal framework for requesting and obtaining digital evidence from abroad in cross-border cases primarily relies on international cooperation mechanisms and domestic legislation. While Nepal does not have specific bilateral treaties or legislation dedicated solely to this purpose, it engages in mutual legal assistance through mechanisms such as Mutual Legal Assistance Treaties (MLATs) and international conventions. MLATs establish procedures for requesting and aiding in criminal matters, including the exchange of digital evidence, while international conventions such as the Budapest Convention on Cybercrime offer frameworks for cooperation in combating cyber threats. However, Nepal has neither executed such bilateral treaties for mutual legal assistance nor has been party to the international or regional legal framework for cooperation in evidence sharing.

According to Mutual Legal Assistance Act 2070 (2014),[19] a document obtained by a foreign state pursuant to the laws of such foreign state and submitted before the court through central authority is considered admissible as evidence in Court when a request for mutual legal assistance is made pursuant to Section 15 of the Act. Upon meeting these conditions, documents may be taken into evidence in accordance with the law. Finally, documents, evidence attached with a request made for mutual legal assistance pursuant to this Act must be certified by the judge or competent government officer and bear the seal of office, otherwise the document shall not be recognized as evidence.[20]

However, Nepal collaborates with organizations like Interpol and participates in regional initiatives to enhance legal cooperation and combat cybercrime. Domestically, Nepal's legal framework, including the Criminal Procedure Code and Evidence Act, provides the basis for admitting digital evidence in court proceedings, though specific provisions for digital evidence from abroad may be lacking. Despite these mechanisms, challenges such as differences in legal systems and resource constraints may impact

19 Section 16 of the MLA Act 2070 (2014).
20 Section 39 of MLA

Nepal's ability to effectively engage in international cooperation for obtaining digital evidence in cross-border cases. [21]

## 3.3 Admissibility of Digital Evidence in Judicial Proceedings of Nepal

**i. Commission for the Investigation of Abuse of Authority versus Prem Bahadur Thapa[22]**

When investigating corruption using espionage, it is necessary to adopt appropriate methods while closely monitoring suspicious individuals, proving the amount seized in case of bribery between any service recipient and government servant, preparing audio-visual evidence through technology, searching for the source of acquired property, conducting scientific collection and examination of evidence. This decision highlights the need of supportive evidences, which can be in digital form for supporting the case presented by the investigating authority.

**ii. Baburam Aryal versus Office of the Prime Minister and Council of Ministers [23]**

Established international telecommunications service providers must ensure the protection of the privacy and confidentiality of individuals and related data when providing any telecommunications service to them. Someone's information cannot be disclosed on the basis of third party's influence or temptation without any specific legal order or formal letter with prior authority. Failure to provide other parties with access to information without specific legal orders or prior authorization may lead to undue pressure or influence on others.

The protection of information stored in a data bank by information service providers, whether pertaining to individuals, organizations, or the government itself, is not only a matter of individual rights and interests but also applies to the rights of the state and security interests. It is necessary for other organs or bodies of the state to also respect and protect such information, along with the executive and its employees, to the extent necessary. Failure to do so would constitute improper or criminal attempts to breach it.

---

21 Mark Kersten, Challenges and Opportunities: Audio-Visual Evidence in International Criminal Proceedings Posted on March 4, 2020, cited on https://justiceinconflict.org/2020/03/04/challenges-and-opportunities-audio-visual-evidence-in-international-criminal-proceedings/

22 Decision No. 10958 - Corruption (Bribery) Part: 64 Year: 2079 Month: Magh Volume: 10 Decision Date: 2078/08/21 442 Decision Date: 2078/08/21, 075-CR-1472

23 Decision Number: 9740 - Appeal / Order Section: 59 Year: 2074 Month: Baisakh Volume: 1 Decision Date: 2072/10/21 7597, Decision Date: 2072/10/21 069-WO-0268

### iii. Rupa Sunwar Versus Krishna Gopal Shrestha, Minister of Education, Science and Technology[24]

In this case, the court has explained about the process by which any online conversation should be presented before the bench.

The court mandated that access to these conversations (i.e. online communication) should be supervised to prevent unauthorized access to other data and personal information. This supervision requires the presence of an officer from the court's information and technology department, an IT expert, and either the applicant, their representative, or their legal counsel during the access process.

### iv. Ram Bahadur Thapa v Commission for the Investigation of Abuse of Authority[25]

The Chapter 9 of the Evidence Act, 1974, states, "Any statement made otherwise than before the court may be proved." The statement made by the parties through oral, written, or conduct can also be considered as evidence. If the matter disclosed is not contrary to the provisions stipulated in the Evidence Act, 1974, Chapter 9(2)(c), then it can be considered as evidence.

There is a need for further guidance from the law regarding the collection and regulation of matters collected through electronic means. In this regard, there may be ambiguity arising from some inadequacies in taking special evidence. However, this does not mean that evidence collected through electronic means, such as CDs, should not be accepted as evidence in the case. The court cannot ignore the unprecedented developments and advancements in the field of science and technology and its relevance to judicial interpretation.

### v. Sita Devi Thakur et al versus Budhani Thakur [26]

This case is related to DNA test report with the use of Identifier kit, where the expert who gave the test report appeared before the court and explained the process in detail, and there was no question in regard to the expertise of the expert. The court has explained that when any suggestion, report has been obtained from concrete and scientific arguments and chemical tests, and the expert has testified the process and verdict and

---

24 077-WO-1236, Certiorari, Supreme Court. The case involves filling application regarding allegations of discrimination and untouchability and the court had issued an interim order directing the investigative authority to restrict their access to mobile conversations strictly between the involved parties.

25 Decision Number: 9880 - Bribery for Receiving a Bribe Section: 59 Year: 2074 Month: Paush Volume: 9 Decision Date: 2073/09/04 7227, Supreme Court, Joint Bench, Decision Date: 2073/09/04, 071-CR-1089, Case: Bribery for Receiving a Bribe

26 NKP 2067, Volume 11, Decision Number 8501

confirmed the report clearly and without ambiguity, such report should be taken as evidence. This interpretation can be broadly applied in cases of other digital evidences as well.

Expert opinion or report, despite not being the sole conclusive evidence (Single Detrimental Evidence) to establish a fact or event, holds significant weight and is considered as a crucial form of evidence when combined with other evidence, such as witness testimonies or party statements.

In addition to being free from dispute, the expertise and proficiency of the expert should ensure that their testimony presented to the court is precise, certain, unambiguous, and unequivocal. Furthermore, when expert opinion is based on conclusions drawn from definite, solid, and scientific arguments and chemical analysis, and when the expert has provided clear and unambiguous testimony and validation of the examination process and findings in court, such a report should be accepted as evidence.

**vi. Nepal Government versus Urmila Bote**[27]

The audio record made by the deceased in front of a police official that has been testified by the police in the court stating that the recording was done by himself before the death, …, such audio record cannot be regarded not to be fall under the definition of dying declaration. This is an example where an audio record has been taken as an evidence i.e. 'dying declaration' by the court, interpreting that when the source of digital evidence can be confirmed, the cour

**vii. Bam Bahadur Basnet versus Nepal Government**[28]

Photos, videos, audio recordings, CDs, and other digital materials serve as evidence. Discrediting their authenticity is not permissible. Each piece of evidence is valid. When digital forms such as photos, videos, audio recordings, CDs, etc., are presented as evidence by one party, and the other party does not refute them, they are accepted as written evidence. In case of disputes regarding such evidence, their authenticity becomes subject to examination. Otherwise, modern forms of written evidence should cautiously be accepted.

**viii. Makhamali Mishra et al versus Laxmi Kumari Mishra (Shrestha)**[29]

In the event of receiving expert report and having affidavit of such expert in court as a witness in regard to authority and accuracy of such report, wherein such report is not seen otherwise by cross

[27] NKP 2078, Volume 11, Decision Number 10773)
[28] NKP 2070, Volume 6, Decision Number 9022)
[29] NKP 2067, volume 10, Decision number 8483

examination, the court shall not invalidate such scientific examination report on legal grounds. Moreover, as per Section 23(7) of the Evidence Act, 2031, the court shall accept the opinion of an expert as evidence that has not otherwise been observed during cross examination.

This case underlines that the evidence of DNA test report which has been testified by the expert who did the test before the court, should be considered valid. The court uses the term 'scientific examination report' to indicate the DNA test report, and this phrase can be widely interpreted to included other scientific data which can be submitted before the court as evidence.

**ix. Ashokram Mahara versus Choteylal Ram**[30]

Expert opinion should certainly assist the judge in reaching a conclusion. However, considering the expert opinion as the only definitive evidence and disregarding other evidence is not justifiable. If the expert opinion is in contradiction to other reliable evidence, the judge may deduce the conclusion against the expert opinion.

**x. Ram Bahadur Basnet versus Nepal Government**[31]

Expert opinion that does not align with the attached evidence or facts should not be considered as valid evidence. Disregarding other evidence in the case file and compelling the judge to accept the expert opinion as mandatory undermines the judge's discretion. In technical matters, the expertise of a specialist in a relevant subject is not easily dismissed. However, if the expert's opinion diverges significantly from the evidence and established facts of the case, causing reasonable doubt, such opinion be rejected. Ignoring the relevant legal provisions or misinterpreting them should not serve as a basis to include the expert opinion as evidence.

The cases mentioned present a comprehensive view of the legal landscape in Nepal, highlighting several crucial aspects of judicial proceedings and legal principles. Firstly, there is a strong emphasis on protecting individual rights and privacy. These cases underscore the importance of conducting investigations within the boundaries of the law and respecting privacy rights, even in the face of crime prevention and detection. Similarly, the Supreme Court's proactive approach to addressing issues of privacy and data protection of the alleged parties during the investigation process. Through its

[30] NKP 2068, Volume 3, Decision Number 8582)
[31] NKP 2065, volume 7, Decision Number 7985

directives, the court seeks to balance the need for thorough investigation with the imperative to respect individuals' rights and maintain the integrity of the legal process.

Secondly, the recognition of electronic evidence, such as CDs and audio recordings, as valid forms of evidence indicate the judiciary's acknowledgment of technological advancements and their relevance in legal proceedings. This recognition reflects the need for clear guidelines on the collection, admissibility, and authenticity of electronic evidence.

Furthermore, the significance of expert opinions in court proceedings is highlighted in multiple cases. Expert opinions are considered valuable when supported by solid evidence and scientific analysis, providing insights that complement other forms of evidence presented in court.

In conclusion, while audiovisual evidence presents opportunities for advancing accountability for mass crimes, its proper collection, preservation, and authentication are essential to ensure its effectiveness in court. As technology continues to evolve, practitioners must remain vigilant in addressing the unique challenges posed by digital and open-source evidence.

Overall, these cases underscore the importance of maintaining a balance between individual rights, technological advancements, and legal principles in the administration of justice in Nepal. They reflect the evolving nature of legal practices and the judiciary's efforts to adapt to modern challenges while upholding fairness, integrity, and the rule of law.

# 4. ADMISSIBILITY OF DIGITAL EVIDENCE IN LAWS

## 4.1 Pre- requisite for admissibility of Digital Evidence

### i. Submitting Digital data as evidence

To ensure that digital evidence is admissible in court, certain legal and technical prerequisites must be satisfied.[32]. Legally, courts scrutinize the authorization for searches and seizures of digital information, as well as the relevance, authenticity, integrity, and reliability of the evidence. Regarding the technical aspect, courts evaluate digital forensics procedures, tools, laboratories, forensic reports, and the qualifications of forensic analysts and expert witnesses. Digital evidence gathered by unauthorized search and seizure could always be challenged as a fruit of a poisonous tree and may be inadmissible in a court of law. Such evidence violates legal standards established to safeguard privacy and ensure fairness in criminal proceedings. Admitting evidence obtained unlawfully undermines public trust in judicial processes, promotes abuse of authority, and establishes a perilous precedent for future investigations. It is therefore crucial to uphold the rule of law and protect individual rights. This approach is necessary to maintain the integrity of the legal system and to protect individual's constitutional rights against unreasonable searches.

### ii. Digital Evidence Assessment

In this phase, courts ascertain whether the proper legal authorization was obtained to search for and seize information and communication technology (ICT) and associated data. This authorization typically comes in the form of a search warrant, court order, or subpoena, and varies depending on national laws and the specifics of the case. While search warrants are commonly used to seize ICT, the requirements for legal orders differ among jurisdictions based on factors such as the circumstances of the case and the qualifications of those conducting the search.

Additionally, the forensic relevance of the digital evidence is evaluated during this phase. This involves determining whether the evidence establishes or disproves connections between the perpetrator and the victim, crime scene, or digital devices. It also involves assessing whether the evidence supports or

[32] Antwi-Boasiako, A., Venter, H. (2017). A Model for Digital Evidence Admissibility Assessment. In: Peterson, G., Shenoi, S. (eds) Advances in Digital Forensics XIII. DigitalForensics 2017. IFIP Advances in Information and Communication Technology, vol 511. Springer, Cham. https://doi.org/10.1007/978-3-319-67208-3_2

contradicts witness testimony, identifies the perpetrator(s), provides investigative leads, sheds light on the perpetrator's methods (modus operandi), and demonstrates that a crime has occurred.[33]

**iii. Digital Evidence Consideration**

In this phase, the integrity of digital evidence is assessed by scrutinizing the digital forensics procedures and tools utilized in obtaining the evidence, as well as the competence and qualifications of the digital forensics experts involved in its acquisition, preservation, and analysis. This evaluation aims to ensure that scientific principles were adhered to in the preservation, acquisition, and analysis of digital evidence, and that standards were met in handling and examining it.

Digital forensics experts present testimony in court to elucidate their qualifications, explain the workings of digital devices and ICT-related sources, outline the digital forensics process, justify the selection of specific digital forensics tools, describe how digital evidence was preserved, acquired, and analyzed, interpret the findings of analyses, assess the accuracy of these interpretations, and account for any alterations to the data and their reasons.

The qualifications of digital forensics experts are also scrutinized to confirm the competency of individuals handling and analyzing digital evidence. This competency is crucial to ensure the quality of work products and install confidence in the results produced. While there are no universal competency standards for digital forensics experts, their qualifications vary by country, and certification may or may not be required depending on the jurisdiction. This phase evaluates whether experts possess the necessary qualifications to act as expert witnesses and/or conduct examinations of ICT and ICT-related data, and whether their competency has been verified and tested.[34]

**iv. Digital Evidence Determination**

In this phase, the authenticity, integrity, and reliability of digital evidence are evaluated based on the assessment conducted in the previous phase. This includes verifying the use of forensically sound methods and tools and relying on expert testimony to confirm the evidence's credibility. Admissible digital evidence must establish relevant facts, remain unchanged throughout the forensic process, and be supported by valid, peer-reviewed results. It's essential that interpretations of findings are unbiased, with any errors or limitations disclosed. Overall, this three-phase model harmonizes legal and technical

33 US National Institute of Justice; 2004a; Maras, 2014

34 Brezinski and Killalea, 2002; US National Institute of Justice, 2004a; European Network of Forensic Science Institute, 2015

standards for digital evidence admissibility across jurisdictions, emphasizing the need for standardized digital forensics practices to combat transnational cybercrime effectively.

## 4.2 Challenges on Admissibility of Digital Evidence

Pre-search and post-seizure warrants are critical components of digital forensic investigations, presenting numerous challenges in the gathering and admissibility of digital evidence in court. If there is no warrant or judicial check mechanism in gathering and investigation of digital evidence that could lead into the investigation being arbitrary, disproportionate and beyond the necessity. The pre-search warrant, issued by the court before investigators arrive at the cybercrime scene, authorizes law enforcement and digital forensics teams to collect evidence. Conversely, the post-seizure warrant requires investigators to document all activities conducted after the seizure to ensure chain of custody. Technical challenges include issues with network security, outdated tools, and a lack of expertise among investigators. Legal challenges arise from the need for authentic, accurate, and convincing evidence, compounded by gaps in cybercrime legislation and enforcement, as well as difficulties in obtaining and executing warrants due to procedural inconsistencies and stakeholder involvement issues. In absence of adequate provisions, digital evidences become questionable regarding their integrity and authenticity. The concerned person may face violation of privacy rights. There will be uncertainty in legal outcomes, and a tendency of admission of unreliable evidences may occur. There can be technological misinterpretations leading to denial of fair opportunity to challenge any evidence against them. International cooperation difficulties may arise when crimes involve multiple jurisdictions where differing rules or absence of rules will undermine the evidentiary value of digital evidences.

### i. Authenticity

In digital forensic investigations, it's critical to ensure that digital evidence remains unaltered and that proper procedures are followed during evidence collection to maintain its usability and admissibility in court. Digital data can exist in various states, such as at rest, active, deleted, hidden, encrypted, or overwritten, all of which may be relevant for litigation purposes and maintaining evidential integrity. In cases of uncertainty, evidence that has been partially overwritten or altered can still be utilized to ensure accurate, reliable, and verifiable findings in accordance with judicial standards.

### ii. Accuracy

Accurate digital forensic investigations require meticulous adherence to legally sound chain of custody protocols, ensuring consistency and integrity of evidence from pre-seizure to post-seizure. This involves thorough documentation of evidence gathering, preservation, and storage procedures, following scientific principles for analysis. Challenges arise in maintaining accuracy throughout the process, often leading to inadmissible evidence in court. To mitigate this, meticulous record-keeping of all activities is essential, including names, dates, times, questions, findings, and assumptions. Preservation methods differ between crime scenes and forensic labs, necessitating distinct approaches. Despite the seemingly invincible nature of digital evidence, examiners must employ legal techniques and tools for discovery. However, ensuring authenticity and accuracy can be compromised due to uncertainties such as system shutdowns during live analysis or tampering during transit in dead analysis.

### iii. Completeness

The digital evidence gathering process necessitates a consistent chain of custody to ensure authenticity and accuracy. Legal requirements demand thorough documentation of exhibit numbers throughout, including investigation procedures, tools, and hypotheses. Peer review by expert witnesses is essential to validate the legality of findings without dispute. Investigators must explain the process used to identify and preserve evidence at crime scenes and labs.

### iv. Convincing

To ensure digital evidence is convincing to the judges, it must meet high standards of acceptability, avoiding interference or doubt. Diligent digital forensic investigation ensures authenticity, accuracy, and completeness of evidence, meeting legal requirements. Evidence should be presented in a non-technical manner, considering diverse backgrounds of the judges and decision makers. Digital evidence clarifies digital events and the development of hypotheses, tested using scientific methods.

# 5. INTERNATIONAL PRACTICES ON RECOGNITION AND REALIZATION OF DIGITAL EVIDENCE

Digital evidence plays a crucial role in criminal investigations and prosecutions across various Asian countries, as highlighted in a research report commissioned by the International Criminal Police Organisation and conducted by The University of Hong Kong.[35]

i. **Bangladesh:** In Bangladesh, case law recognizes video and audio recorded evidence as falling within the definition of "document" under the Evidence Act (1872). The Speedy Trial Tribunal Act expressly admits electronically recorded evidence, but the court cannot convict the accused on this evidence alone. The Information and Communication Technology Act (2006) (ICTAB) and the Digital Security Act (2018) (DSAB) were enacted to address cybercrime in Bangladesh. The ICTAB clarifies that a statement recorded digitally in electronic form qualifies as a written statement under the Evidence Act. The DSAB put in place procedures to regulate the forensic investigation of digital evidence. The Cyber Tribunal, created by the ICTAB, can admit "forensic evidence" obtained or collected under the DSAB.

ii. **Bhutan:** The definition of "evidence" in Bhutan's Evidence Act (2005) includes electronic documents and records. The court may decline to admit an electronic document if a genuine question is raised as to the security or integrity of the electronic document system used to record or store the document. Though hearsay evidence is inadmissible, the court has wide discretionary powers to admit hearsay. The Information, Communications and Media Act (2018) confers legal recognition on data messages and electronic documents.

iii. **Brunei:** In Brunei's Evidence Act (2014 edition) the definition of "document" includes any matter recorded, stored, processed, retrieved, or produced by a computer. Though hearsay evidence is inadmissible, both the Evidence Act and the Computer Misuse Act (2007 edition) allow for the admission of statements produced by a computer to prove the truth of the contents, under certain conditions. In assessing the weight to be given to a document produced by a computer, the court should consider all of the circumstances, including whether the information was supplied to the computer contemporaneously with

[35] Interpol, The Use of Digital Evidence in Prosecution in Asia, A Comparative Study on the laws and policies governing the admissibility and use of digital evidence in criminal proceedings in Bangladesh, Bhutan, Brunei, Cambodia, Maldives, Mongolia, Nepal, Srilanka and Vietnam

the occurrence of the facts the information describes, and whether the person who supplied the information had any incentive to conceal or misrepresent the facts.

iv. **Cambodia:** Cambodia's Code of Criminal Procedure states that all evidence is admissible unless provided otherwise in law. The Law on Electronic Commerce (2019) provides that digital evidence shall not be rejected in legal proceedings on the sole grounds that the evidence is in the form of an electronic record. A draft Cybercrime Law has yet to be enacted. One decision of the Extraordinary Chambers in the Courts of Cambodia excluded film footage of an alleged interrogation centre because the evidence was repetitive and would have required lengthy investigations into its authenticity.

v. **Maldives:** Although the Maldives Evidence Act (1976) has yet to be updated, the courts will still allow digital evidence when relevant under the terms of this act. A new evidence bill, which provides for the admission of digital evidence, is currently before Parliament.

vi. **Mongolia:** Mongolia's Criminal Procedure Law (2002) provides that facts and information regarding the circumstances of a crime shall be deemed to be evidence if obtained in accordance with this law. The law recognises audio and video recordings (including photos obtained or produced from these recordings) as "documents", and electronic recordings can be used to corroborate the evidence.

vii. **Sri Lanka:** Sri Lanka's Evidence (Special Provisions) Act (1995) provides for the admissibility of digital evidence such as audio-visual recordings and statements produced by computers. The Electronic Transactions Act (2006) further provides for the admissibility of information contained in a data message, electronic document, electronic record, or other communication. Both laws have provisions allowing the court to presume the accuracy or truth of information contained in an electronic document or record unless the contrary is proved. The Computer Crime Act (2007) created new cybercrime offences and powers to obtain computer data.

viii. **Vietnam:** Vietnam's Criminal Procedure Code (2015) recognizes "electronic data" as a source of evidence. The same law has specific rules for acquiring, storing, preserving, copying, restoring, and displaying electronic data. The findings of expert examinations may be used to explain and present digital evidence. The Law on E-Transactions (2005) provides for the legal validity of data messages.

These countries demonstrate varying degrees of readiness in incorporating digital evidence into their legal systems, with ongoing efforts to update legislation and enhance capabilities for handling digital evidence in criminal cases.

Following best practices of legality of search and seizure of digital evidence is worth discussion.

**a. India**

In India, there is no law regulating the field of search and seizure of electronic devices in a criminal investigation. In case of *Virendra Khanna v. State of Karnataka,* the High Court of Karnataka[36], discussed the legislative framework under section 69(1) of Information Technology Act, 2000 where court laid down the detailed procedure to unlock the digital devices and email address. As per the directive given by the court, firstly, the investigating officer may request or give direction to provide passwords, biometrics etc. Alternatively, the officer can approach a court for a search and seizure order. The last resort in the process is hacking after procuring the court's order. Court stipulated that failure of the procedure leads to a negative presumption against the accused. On 7th November 2023, the Supreme Court of India issued a comprehensive guidelines for search and seizure of digital devices for protection of right to privacy which was the result of a petition filed by the Foundation of Media Professionals, a journalist group.[37] Recently on 5 January 2024, the Supreme Court of India issued a notice to investigative agencies and the Delhi police on a petition filed by online portal where court has highlighted the lack of transparency and formal procedure when personal digital devices of journalist are seized during the raids[38].

**b. United States of America**

The concern of privacy and legitimate search and seizure of digital device was addressed by Supreme Court of USA in *Riley v. California* and *US v. Wurie* on 29 April 2014[39]. The debate revolves around whether police can search individuals' cell phones without a specific warrant after their arrest, especially when arrested for minor offenses. In some cases, such warrantless searches have uncovered evidence leading to more serious convictions. The appeal seeks to suppress this evidence, arguing it violates the Fourth Amendment of the U.S. Constitution, which protects against unreasonable

[36] Virendra Khanna v. State of Karnataka, High Court of Karnataka, WP 11759/2020, Decided on March 12, 2021.

[37] https://www.scobserver.in/journal/guidelines-for-search-and-seizure-of-digital-devices-a-must-under-right-to-privacy-supreme-court-says/

[38] https://www.thehindu.com/news/national/sc-notice-on-newsclick-plea-for-guidelines-on-seizure-of-digital-devices/article67709600.ece

[39] https://cis-india.org/internet-governance/blog/search-and-seizure-and-right-to-privacy-in-digital-age#fn1

searches and seizures. The challenge lies in defining what constitutes "unreasonable" without clear guidelines, leading courts to interpret on a case-by-case basis. The Fourth Amendment protects against unwarranted government intrusion, generally considering warrantless searches unreasonable unless exceptions apply. This protection is subjective, based on an individual's reasonable expectation of privacy rather than the physical location being searched.

Regarding electronic devices in the USA, law enforcement typically needs a search warrant before accessing them, especially when these devices are stored in private locations like homes or workplaces. Generally, searches of homes require warrants due to the inherent expectation of privacy. In 2014, the U.S. Supreme Court ruled that digital devices cannot be searched without a warrant or owner's consent. These devices contain vast private information distinct from items like wallets. If a digital device is seized during a standard search, law enforcement must preserve it until a proper warrant is obtained to search its contents.[40]

For a warrant to be valid, it must meet specific criteria: probable cause of evidence related to a crime, an oath from the requesting officer, detailed description of items to be searched, and approval from an unbiased judge. The warrant doesn't automatically grant authority to search electronic devices found inside. If there's a suspicion of crime-related evidence on an electronic device within a home, it must either be included in the initial warrant or a separate.

[40] https://www.pumphreylawfirm.com/blog/search-and-seizure-of-computers-in-criminal-cases/

# 6. GENERAL OBSERVATION OF DIGITAL EVIDENCE COLLECTION PROCEDURE IN NEPAL

### Collection and Seizure of Electronic Devices

As a matter of practice, when law enforcement officials harbor suspicions or receive secret information, they often promptly seize electronic devices from the suspects. The suspects are presented with an arrest warrant obtained either from the court or an emergency arrest warrant in accordance with the law. Once apprehended, law enforcement officials methodically follow procedures of search and seize instruments pertinent to the ongoing investigation. This process adheres to specific procedures outlined in general criminal procedural laws and specialized laws, such as those related to narcotics cases nevertheless there is no hard and fast rule relating to digital evidences and the devices, even when not-associated with the crime are seized and all access to private and non-warranted digital data is cut off from the accused.

### Examination of Digital Content

Post-seizure, law enforcement officials record the seizure of electronic evidence, taking not just the physical device but also its electronic content for examination. Surprisingly, there is no court warrant requirement to delve into the details of the electronic content of the seized device. Despite the Supreme Court of Nepal emphasizing privacy rights and mandating court warrants for call details and location data, there exists no specific guideline concerning the realization of digital evidence. Devices sent for investigation lack regulation or specific protocols. This absence of protocol denies the data subject (suspect) an opportunity to consent to the investigation of their devices, leading to potential self-incrimination. Such practices seem to contradict the fundamental rights guaranteed by the Constitution of Nepal, which prohibit self-incrimination. Moreover, during the seizure of digital evidence, suspects are often required to provide security patterns or lock codes for their digital devices, which further violates the principle of self-incrimination. The practice of examination of digital evidences have evolved without proper rules to guide them, and traditional process of examination have been interpreted to cover the procedure of examination of digital evidence. Even though it has been contended by the investigating authority time and again that a judicial warrant for collecting digital evidence creates a backlog of cases, nevertheless, this cannot be accepted as a basis of denial of constitutional rights. Therefore, there is a sheer necessity to create effective legal mechanisms which

extend the scope of prevailing guidelines for forensic labs in Nepal and elaborates the procedure to be observed by the law enforcement for examining digital evidences.

### Issues of Necessity, Proportionality, and Judicial Warrant

There may be instances where law enforcement authorities' investigations into digital devices exceeded the bounds of necessity, proportionality, and the requirement for a judicial warrant. Notably, Nepalese laws do not explicitly provide for a judicial warrant in such investigations, rendering law enforcement's actions somewhat arbitrary. While a judicial warrant is mandatory when obtaining call details and user location from telecom operators, no such requirement exists for obtaining personal information from social networking providers. Consequently, law enforcement agencies frequently access personal data from platforms like Meta and X without proper procedural guidelines, potentially infringing on privacy rights. Due to lack of proper procedural guidelines for the judicial authority or data controllers' approval for such information, there have been instances where the investigation officials' act has been beyond the necessity, being disproportionate and infringement on the privacy without the legislative enactment.

### Procedural Errors and Arbitrary Investigations

In a specific case of cheating, a suspect was arrested due to a complaint about a WhatsApp conversation. During the investigation, the focus shifted arbitrarily, revealing an app related to cryptocurrency trading on the suspect's device. As a result, a new case was initiated against the suspect based on this discovery. While law enforcement authorities may have acted in good faith, their procedural errors raise significant questions. Although as discussed above, Supreme Court has emphasized the need to regulate the realization of digital evidence to prevent arbitrary investigations, it has not been taken seriously and discussed for proper review. There is a widespread concept rooted in the law enforcement officials that privacy approach cannot supersede the protection approach while investigating serious offences. This scenario of individual officials working on the basis of their own opinions and interpretations has been created due to the government's lack of attention towards maintaining procedural fairness and preparing extensive guidelines for collection, processing, submission and evaluation of digital evidence. The court has been often observed to have turned a blind eye towards arbitrary approaches undertaken by the investigating authority, procedural flaws and lack of proper procedural and technical resources in the court itself. This situation poses a perilous threat to the entire criminal justice system of Nepal, therefore it is essential to create a framework

which addresses the process of collection, examination, submission and evaluation of digital forensic evidence .

### Forensic Examination and Issues of Authenticity

Forensic examinations of digital devices in Nepal are predominantly conducted by the Nepal Police's forensic department. Suspects or defendants have no legal basis to conduct or request for independent digital forensic examinations of devices seized by the police. This exclusive control over forensic examinations by the police undermines the principle of equality of arms in the criminal justice system, which is essential for a balanced and just criminal justice system. Additionally, the lack of standardized protocols for digital evidence collection and examination raises concerns about evidence tampering and authenticity.

### Security and Protection of Digital Evidence

Despite the importance of digital evidence, Nepal lacks legal provisions and procedures for its protection. Digital evidence, including logs and trails, is often stored for limited periods without proper backup procedures or security measures, posing risks to its integrity during court proceedings.

### Qualifications and Expertise in Digital Forensics

Digital forensic examinations in Nepal are conducted by technocrats within the police organization, without explicit statutory or legal requirements regarding their qualifications and expertise. This lack of standardized qualifications can lead to challenges regarding the credibility and admissibility of forensic reports in court.

### Security Concerns and Content Protection

Digital evidence submitted to courts often remains insecure, stored on the same digital devices without proper wiping. This lack of security risks unauthorized access to sensitive information, potentially compromising the integrity of the evidence and victims' privacy. The digital evidence gathered by investigators are submitted to the court in the same digital device without completely wiping the device. And the cases remain sub-judice in court for many years. During the court proceedings the security of those digital devices is not maintained. Any of the court officials has easy access to those devices and content thereof. Once the case is finished, in case of defendant being acquitted, the defendant will receive the device back. But in case if the defendant is held by the court and court

orders for confiscation of those devices, the devices are sold in the open market without taking care of the content therein. When sold in the open market without completely wiping out, the content of those devices are easily forwarded to other general people making the content at risk of being in access to other people and the victim being re-victimized.

Therefore, while digital evidence is crucial in modern-day criminal investigations, Nepal faces numerous challenges in its collection, handling, and presentation. To ensure justice, fairness, and the protection of individuals' rights, Nepal urgently needs to address these issues by establishing clear guidelines, standardized protocols, and ensuring the qualification and expertise of those involved in digital forensic examinations. Only by addressing these challenges can Nepal enhance the credibility, admissibility, and reliability of digital evidence in its legal system.

# 7. RECOMMENDATIONS

While Nepal has made strides in recognizing and incorporating digital evidence into its legal system and practices, there are significant challenges to address. By adopting these recommendations and continually adapting to technological advancements and global best practices, Nepal can strengthen its legal framework, enhance the credibility and admissibility of digital evidence, and ensure justice, fairness, rule of law and respect for individuals' rights in its legal system. The prominent problems faced by individuals under investigation include violation of their personal privacy, unreasonable seizure of not only their personal devices but also their personal data, obstacles in getting back their personal devices after completion of investigations etc.

**Establish Clear Guidelines and Protocols**

It is a dire necessity to develop comprehensive and clear statutory guidelines specifically tailored to the collection, handling, and examination of digital evidence. There is also a requirement of implementation of standardized protocols to ensure consistent and lawful procedures are followed by law enforcement officials during the seizure, examination, and storage of digital devices and data. A robust mechanism considering the societal situation and existing challenges should be developed for ensuring a lawful and just process of collection, examination, admission and evaluation of digital evidence where a proper chain of command exists throughout investigative and judicial processes so that every individual feels safe in the hands of the judicial system.

**Chain of Custody Protocols**

It is recommended to implement strict protocols for maintaining the chain of custody of digital evidence from collection to presentation in court. This includes documenting every step of evidence handling, storage, and access to prevent tampering and ensure its integrity. The person deriving the digital evidence should be of specific qualification and designation that is capable of maintaining the chain of custody. The prevailing guidelines applicable to forensic labs and law enforcement only cover the chain of custody of digital evidence during their examination process; however, chain of custody should be maintained throughout the judicial process and inside the courts as well to protect the integrity and confidentiality of personal data.

**Mandatory Judicial Oversight**

Considering the best practices globally and also constitutional provision and precedent of Supreme Court of Nepal there is urgent requirement to introduce a legislation requiring judicial warrants for the search and examination of digital content, ensuring that investigations remain within legal boundaries and respect individuals' privacy rights and judicially checked. Furthermore, the judicial consent mechanism that is practiced in context of call detail and user location should also be adhered while obtaining personal information of any person from any company inside and outside the territory of Nepal. There should be an establishment of clear criteria for when and how such warrants can be obtained, emphasizing the principles of necessity, proportionality, and respect for human rights along with procedural flexibility and exemption in case of national interest and emergency.

**Enhance Data Subject Consent and Rights**

It is further recommended to enact laws that empower data subjects (suspects) to give informed consent for the investigation of their digital devices, ensuring they are aware of their rights and potential implications. Furthermore, it is suggested to strengthen legal provisions to protect individuals against self-incrimination, prohibiting law enforcement from compelling suspects to provide security patterns or lock codes for their digital devices.

**Improve Digital Forensic Practices**

It is recommended to implement legal requirements for digital forensic examiners to possess recognized qualifications and expertise, ensuring the credibility and admissibility of forensic reports in court. It is further recommended to invest in training programs and certifications for digital forensics experts to ensure they possess the necessary skills and knowledge. Standardizing qualifications can improve the credibility and reliability of forensic examinations. Furthermore, to balance the arms of parties of the case, it is also recommended to establish independent bodies or agencies responsible for conducting digital forensic examinations, separate from law enforcement agencies, to ensure impartiality and avoid conflicts of interest.

**Enhance Data Protection and Security**

It is further recommended to introduce legal provisions mandating the secure storage, backup, and protection of digital evidence, including logs, trails, and other pertinent data. It is also recommended to develop mechanisms to safeguard digital evidence during court proceedings, ensuring its integrity and preventing unauthorized access or tampering. Furthermore it is recommended to utilize

encryption, digital signatures, and other authentication techniques to enhance the integrity and credibility of digital evidence.

**Prioritize Necessity, Purposiveness, and Proportionality**

It is recommended to emphasize the importance of considering the necessity, purposiveness, and proportionality of digital investigations. Furthermore, it is also recommended that the digital evidence governance system must ensure that investigative actions are justified, targeted, and proportionate to the objectives, minimizing unnecessary intrusion and respecting individuals' rights.

**Ensure Admissibility and Reliability of Evidence**

It is recommended to provide clear guidance on the admissibility and reliability of digital evidence, including photos, videos, audio recordings, CDs, and expert opinions. There should also be adherence to established legal standards and verification processes will enhance the credibility of evidence presented in court proceedings.

**Improve Public Awareness and Training**

It is also recommended to conduct public awareness campaigns and training programs for law enforcement officials, legal professionals, and the general public on the importance, legal frameworks, and best practices related to digital evidence. It is also recommended to foster collaboration between relevant stakeholders, including government agencies, legal experts, technologists, and civil society organizations, to exchange knowledge, share experiences, and develop innovative solutions to emerging challenges in digital evidence.

**Review and Update Existing Legislation**

It is recommended to regularly review and update existing laws and regulations related to digital evidence to address emerging technological advancements, global best practices, and evolving human rights standards. It is further suggested to ensure that new legislation is consistent with international standards, human rights principles, and Nepal's constitutional guarantees, including the right to privacy, freedom from self-incrimination, and equality before the law.

**Establish Accountability Mechanisms**

It is recommended to implement robust accountability mechanisms to monitor and evaluate the implementation of digital evidence laws and practices, ensuring compliance with legal requirements, ethical standards, and human rights principles. Furthermore, it is also required to establish independent oversight bodies or mechanisms to investigate complaints, misconduct, or abuses related to the collection, handling, and use of digital evidence, and to hold accountable those responsible for violations or breaches of the law.

**International Cooperation**

It is recommended to strengthen international cooperation mechanisms, such as mutual legal assistance treaties and collaborations with organizations like Interpol, to facilitate the collection and admissibility of digital evidence in cross-border cases by undergoing bilateral or multilateral treaty arrangements.

# BIBLIOGRAPHY

Antwi-Boasiako, A., Venter, H. (2017). A Model for Digital Evidence Admissibility Assessment. In: Peterson, G., Shenoi, S. (eds) Advances in Digital Forensics XIII. DigitalForensics 2017. IFIP Advances in Information and Communication Technology, vol 511. Springer, Cham. https://doi.org/10.1007/978-3-319-67208-3_2

Brezinski and Killalea, 2002; US National Institute of Justice, 2004; European Network of Forensic Science Institute, 2015

Council of Europe, *Convention on Cybercrime* (ETS No. 185), opened for signature Nov. 23, 2001

Criminal Code of Nepal

Criminal Procedure Code

Decision No. 10958 - Corruption (Bribery) Part: 64 Year: 2079 Month: Magh Volume: 10 Decision Date: 2078/08/21 442 Decision Date: 2078/08/21, 075-CR-1472

Decision Number: 9740 - Appeal / Order Section: 59 Year: 2074 Month: Baisakh Volume: 1 Decision Date: 2072/10/21 7597, Decision Date: 2072/10/21 069-WO-0268

Decision Number: 9880 - Bribery for Receiving a Bribe Section: 59 Year: 2074 Month: Paush Volume: 9 Decision Date: 2073/09/04 7227, Supreme Court, Joint Bench, Decision Date: 2073/09/04, 071-CR-1089, Case: Bribery for Receiving a Bribe

Digital Evidence and the New Criminal Procedure Author(s): Orin S. Kerr Source: Columbia Law Review , Jan., 2005, Vol. 105, No. 1 (Jan., 2005), pp. 279-318 Published by: Columbia Law Review Association, Inc. Stable URL: https://www.jstor.org/stable/4099310

Duranti, Luciana, and Allison Stanfield. "Authenticating Electronic Evidence." *Electronic Evidence and Electronic Signatures*, edited by Stephen Mason and Daniel Seng, CMB-Combined volume, 5, University of London Press, 2021, pp. 236–78. *JSTOR*, http://www.jstor.org/stable/j.ctv1vbd28p.13. Accessed 27 Mar. 2024

Electronic Transactions Act

England and Wales care Standards Tribunal, Mogford v Secretary of State for Education and Skills [2002] EWCST 11(PC) (26 June 2002)
https://www.bailii.org/ew/cases/EWCST/2002/11(PC).html
https://cis-india.org/internet-governance/blog/search-and-seizure-and-right-to-privacy-in-digital-age#fn1
https://www.pumphreylawfirm.com/blog/search-and-seizure-of-computers-in-criminal-cases/
https://www.scobserver.in/journal/guidelines-for-search-and-seizure-of-digital-devices-a-must-under-right-to-privacy-supreme-court-says/
https://www.thehindu.com/news/national/sc-notice-on-newsclick-plea-for-guidelines-on-seizure-of-digital-devices/article67709600.ece
Interpol, The Use of Digital Evidence in Prosecution in Asia, A Comparative Study on the laws and policies governing the admissibility and use of digital evidence in criminal proceedings in Bangladesh, Bhutan, Brunei, Cambodia, Maldives, Mongolia, Nepal, Srilanka and Vietnam
ISO/IEC 27042: ISO/IEC JTC 1/SC 27, *Information Technology—Security Techniques—Guidelines for the Analysis and Interpretation of Digital Evidence*, ISO (Year varies)

ISO/IEC JTC 1/SC 27, *Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence*, ISO (2012), available at, https://webstore.ansi.org/preview-pages/INCITS/preview_INCITS+ISO+IEC+27037+2012+(R2019).pdf?srsltid=AfmBOoqREc1Pliql6CQCOGXgN4J0S3mPjdSRt9Ib_XYJjPLL1Yf8zWG_

Jason Liser Plaintiff v. Jeffrey Smith et al, United States District Court, D. Columbia, No. CIV.A.00-2325 (ESH) (D.D.C. Mar. 26, 2003)

Kersten Mark , Challenges and Opportunities: Audio-Visual Evidence in International Criminal Proceedings

Mason, Stephen, et al. "Proof: The Technical Collection and Examination of Electronic Evidence." *Electronic Evidence*, edited by Stephen Mason and Daniel Seng, 4th ed., University of London Press, 2017, pp. 285–338. *JSTOR*, http://www.jstor.org/stable/j.ctv512x65.16. Accessed 27 Mar. 2024

MLA Act 2070 (2014)

NKP 2065, volume 7, Decision Number 7985

NKP 2067, volume 10, Decision number 8483

NKP 2067, Volume 11, Decision Number 8501

NKP 2068, Volume 3, Decision Number 8582)

NKP 2070, Volume 6, Decision Number 9022)

NKP 2078, Volume 11, Decision Number 10773)

Posted on March 4, 2020, cited on https://justiceinconflict.org/2020/03/04/challenges-and-opportunities-audio-visual-evidence-in-international-criminal-proceedings/

Posted on March 4, 2020, cited on https://justiceinconflict.org/2020/03/04/challenges-and-opportunities-audio-visual-evidence-in-international-criminal-proceedings/

Prosecutor v. Thomas Lubanga Dyilo, Case No. ICC-01/04-01/06, Judgment Pursuant to Article 74 of the Statute, Int'l Crim. Ct. (Mar. 14, 2012), available at : https://www.icc-cpi.int/sites/default/files/CaseInformationSheets/LubangaEng.pdf

*Stanford International Bank Limited (in liquidation) v. Hamilton-Smith,* High Court (Antigua), See : https://ag.vlex.com/vid/alexander-m-fundora-applicant-805812073

The Prosecutor v. Jean-Pierre Bemba Gombo, Case No. ICC-01/05-01/08, Judgment Pursuant to Article 74 of the Statute, Int'l Crim. Ct. (Mar. 21, 2016), available at: https://www.icc-cpi.int/sites/default/files/CaseInformationSheets/BembaEng.pdf

United States Court of Appeals, Tenth Circuit, 9 F.3d 823 (10th Cir. 1993)

US National Institute of Justice; 2004a; Maras, 2014

Virendra Khanna v. State of Karnataka, High Court of Karnataka, WP 11759/2020, Decided on March 12, 2021

Williams, Janet. "Acpo good practice guide for digital evidence." *Metropolitan Police Service, Association of chief police officers, GB* (2012): 1556-6013., *Good Practice Guides for Digital Evidence*

Wilson, Nigel, et al. "Proof: The Technical Collection and Examination of Electronic Evidence." *Electronic Evidence and Electronic Signatures*, edited by Stephen Mason and Daniel Seng, CMB-Combined volume, 5, University of London Press, 2021, *JSTOR*, http://www.jstor.org/stable/j.ctv1vbd28p.16. Accessed 27 Mar. 2024

## SUPPORT OUR WORK! DONATE!

Human Rights and Justice Center
Sunrise Bank Ltd 0020388247701001

## VISIT US

Jwagal-10, Kupondole,
Lalitpur, Nepal


+977 9819033495

contact@hrjc.org.np

https://www.hrjc.org.np

https://tinyurl.com/2ym9byf2

https://www.facebook.com/HRJCNepal/


FIND US ON GOOGLE MAPS