UCP Journal *of* Law & Legal Education
Vol. 4, Issue 1 (January – June 2026)

International Perspectives on Digital Forensics Legislation

Syed Shaharyar Ahmed*

Abstract

As technology changes across the globe, the demand for uniform legal structures has become equally crucial. The domain of digital forensics has become more relevant than ever, owing to the differing treaties and nationalised legislation through which it is governed. This paper discusses the legal structures of some selected countries such as the USA and South Africa and some countries from the European Union. These countries were chosen because of the complicated procedures involved in the handling of cross-border digital evidence. The paper attempts to analyse ever-changing digital forensic laws in different jurisdictions and what these mean in the context of having international cooperation in the fight against cybercrime. It underscores the legal contradictions and their effect on the need for mutual legal assistance treaties and elaborates on the relevance of international agreements such as the Budapest Convention on cybercrime. In addition, the paper attempts to analyse the ethical dilemmas dealing with the collection of digital evidence and the requirement to establish a proper chain of custody for the evidence to be admissible in court. This research seeks to assist legislators in devising effective digital forensic policies so that the gaps in the existing legislation and procedures concerning such evidence are addressed. Lastly, this research highlights the need for global cooperation in developing requisite policies governing digital forensics, which meet technological changes and improve the efficiency of digital forensic investigations.

Keywords: Digital Forensics, Cybercrime, Digital Evidence, Forensic Investigation.

* Litigation Associate, Ibrar Law Associates, Lahore, Pakistan. Email: shaharyargcu@gmail.com

Article History: Received: 05-05-2025; Received in revised form: 09-06-2026; Accepted: 21-09-2026.
Available online: 26-10-2026
DOI: https://doi.org/10.24312/ucp-jlle.04.01.534

OPEN ACCESS

Introduction

The growing use of technology has exacerbated issues surrounding cybercrime and the regulation of digital forensics. States are attempting to grapple with the cross-border nature of digital evidence and the rapid developments in technology that outpace legal instruments designed to govern them (Casey, 2010). This paper surveys the legislation on digital forensics from an international perspective, including the United States, South Africa, and European Union member states. It seeks to identify the most important obstacles to international cooperation in the prosecution of cybercrime and offer solutions to improve the movement of digital evidence across borders. As technology becomes more globalised, the rate of cybercrime skyrockets, often extending beyond the borders of an individual nation (Casey, 2010). As a result, the need for an even more coherent legal framework that will streamline the collection, preservation, and presentation of digital evidence in a court of law is more critical than ever (Chung et al., 2017).

The Budapest Convention on Cybercrime was adopted in 2001 by the Council of Europe, and it is by far the most important legal instrument that addresses the problems concerning cybercrime on a global level. This treaty was enacted to foster international cooperation to fight cybercrime by harmonising criminal provisions on the illegal access to and interference with computer systems and data, along with the misuse of electronic devices. This treaty also mandates international cooperation for the purpose of obtaining electronic evidence through law enforcement agencies, which facilitates such access. The Budapest Convention, which acts as a reference point, has aided several countries in developing legal approaches towards the prevention of cybercrime and conducting digital forensics. In response to the Budapest Convention, many countries have drafted their own national laws for incorporating such liberal reforms (Nguyen & Golman, 2020).

Concerns regarding the admissibility of digital evidence in court are another issue which comes with the lack of uniform methods for the acquisition and storage of digital evidence. For instance, various states deploy different legal definitions as to what makes evidence-gathering techniques acceptable or not (Casey, 2011). The ethical implications regarding the gathering of digital

evidence as well as the importance of preserving the chain of custody will be discussed later in this paper. The management of digital evidence is essential, as any distortion in handling this evidence might result in shattering the validity and credibility of such evidence in a court of law. Therefore, fostering clear definitions and best practices for digital forensic investigations is crucial (Alshumrani et al., 2023).

The objective of this research is to suggest effective digital forensics policies and to construct a comprehensive model which addresses the gaps in both legal and procedural frameworks. The Budapest Convention should be relied on by states for promoting inter-state collaboration, and mutual legal assistance treaties should be worked on in order to better prepare the states to fight cybercrime. This research emphasises the need to establish inter-state collaborative action that responds to the pace of technological change for improving digital forensic investigations. This goal will be accomplished by analysing gaps in collaborations and best practices in international cooperation. Using the results of the comparative analysis and stakeholder consultation, formulate strategies to improve digital forensics legislation at the international level. These strategies will seek to respond to existing problems while providing a flexible approach to future developments in technology.

There are still notable gaps in research concerning the legislation on digital forensics that impede the construction of coherent legal systems and policies at the global level. With the relentless evolution of cybercrime, there is a pressing need to have flexible and all-encompassing legislation. This paper intends to pinpoint these gaps and provide an explanation with an emphasis on the global context, which works towards formulating laws on digital forensics. A lack of comparative studies that look at different jurisdictions and their digital forensics legislation is one of the gaps in current research. Some countries have strong laws concerning digital evidence, while others are extremely behind, which makes analysing other countries much more important (Mouhtaropoulos et al., 2014). For example, the literature available focuses too heavily on national law without considering an interdisciplinary approach. This lack of a bigger picture shows how legal systems miss out on the opportunity to optimise operations based on best practices from each other. The lack of comparative analysis makes it difficult to

evaluate what legislative measures are effective and what kinds of reforms are needed (Mohammed et al., 2019).

It is necessary for research to create standards which could be globally accepted throughout various legal cultures and contexts (Beebe, 2009). A significant hurdle in establishing efficient digital forensics legislation is the deficit in comprehending technology and cybercrimes. Many law enforcement officers and legal practitioners do not possess adequate knowledge and skill set concerning digital forensics, owing to which they cannot effectively investigate and deal with the prosecution of cybercrimes. Curing this defect mandates legislation which aims to provide professional training and education to help law enforcement officers and legal professionals deal with advanced digital environments. (Garfinkel, 2010). The ongoing development of technology is a consistent concern for lawmakers who need to respond to emerging cyber threats. Therefore, current laws are usually behind technological developments, and there is always a plethora of gaps which lawmakers need to resolve. More focus should be shifted towards designing rapid and flexible laws for the prevention of cybercrime, while accepting new technology at the same time (Beebe, 2009).

Understanding ways to enhance international cooperation in digital forensic laws has been overlooked for some time. Cybercrime is international in scope and typically requires a multinational response. There is a shortage in the literature addressing the international digital forensic collaborations that deal with the promises, pacts, and frameworks that ensure their establishment, and the barriers that sustain them (Klasén et al., 2024). This paper aims to address that -

How do divergent national legal frameworks and procedural standards impact the cross-border collection, authentication, and admissibility of digital forensic evidence, and what unified legal mechanisms can harmonise global cybercrime investigations while safeguarding fundamental privacy rights?

Research Methodology

This research utilises qualitative methods and relies on doctrinal and functional comparative legal research techniques. The doctrinal component involves a comprehensive study of international agreements and national laws and case law on the

international legal framework on the access, preservation, and custody of digital evidence. This study assesses the flexibility of legal doctrines in response to mutable digital phenomena and the technologies that bring them about. For this study to be methodologically sound, countries were selected with the following characteristics: a country with a different legal system; a country with a different level of technology and law; and a country that is geographically located in the pathways of international data flow. The United States represents a mature common law framework driven by statutory regimes like the Electronic Communications Privacy Act (1986) and the Clarifying Lawful Overseas Use of Data Act. The European Union is a civil law system that provides comprehensive privacy and data protection in the General Data Protection Regulation and a cross-border evidence framework in the e-Evidence Regulation. South Africa is a mixed legal system and is in the process of establishing digital forensics with the Cybercrimes Act. The rapidly digitising economies of the Asia Pacific and the Middle East and North Africa regions are in the process of modernising their laws, and are included for their legislative and structural shortcomings. A functional comparative framework is the basis for this study and regards the various systems and the problem of obtaining and the lawful inclusion of digital evidence in judicial processes while upholding the rights of individuals. The goal of this research is to assess the legal frameworks of multiple countries and describe their key commonalities and trends. This step includes the legal content analysis of policies and other documents and publications to harvest necessary information. After the description phase, the research will begin the analytical integration of the data which have been collected during the description phase. This will analyse how jurisdictions respond to the challenges posed by privacy rights, the protection of personal data, and the challenges of the admissibility of digital evidence and the challenges posed by digital forensic science. This analysis will examine the effects of these laws on the practice of law and on the rights of the individual. The doctrinal method will explore the theories and doctrines of the laws of digital forensics. This method involves the scrutiny of legislation, case law, and the literature to ascertain the functionality of the law. This aims to delineate how legal systems are able to adapt to the challenges posed by technology. Finally, within the operational context, the first focus of research is to present a short

overview of the concept of Digital Forensics. The second focus of research is to describe the various laws on digital forensics and their implications. The last focus of research is to present the different global viewpoints on digital forensics laws and to offer possible improvements and suggestions to enhance the effectiveness of the laws on digital forensics.

Literature Review

Recent studies note that digital transformation impacts criminal investigations and call for flexible forensic frameworks. Artificial Intelligence (AI), Internet of Things (IoT), and the use of cloud infrastructure will increasingly be employed by perpetrators of crime (Beebe, 2009). Therefore, digital forensic frameworks need to expand rapidly and increase analytical capacity. Most scholars argue that AI can automate data analysis and that law enforcement and judicial officers must be trained to assess digital evidence. Klasén et al. (2024) elaborated on the consequences of digital transformation on crime and the dire need for advancements in approaches to digital forensics so that new problems could be tackled. Emerging technologies, for instance, AI, IoT, and drones have started facilitating new genres of crime. The authors have stressed proactive reforms in the arena of digital forensics (Mohammed et al., 2019). This involves reforming digital forensics to significantly enhance both capability and pace, in order to meet the growing demands. Furthermore, police investigators and courts are now becoming increasingly reliant on digital experts to navigate the complexities of digital evidence. Even the public and smaller entities often lack clear guidance on how to handle sensitive data and respond to incidents pertaining to digital crimes, which leads to the loss of valuable digital evidence and hence digital forensics cannot be performed (Klasén et al., 2024). Therefore, the authors suggested that crime investigators and judges should be trained properly to correctly appreciate digital evidence (Klasén et al., 2024).

Clough (2019) analysed the Budapest Convention on Cybercrime and its relevance in the harmonisation of laws related to cybercrime. The author mentioned that coordinated international action is required against the growing threat of cybercrime since the advancements in Information and Communication Technologies

(ICT) have made it quite complex. The Budapest Convention calls for collaboration between law enforcement agencies to combat cross-border cybercrime under Article 35. For effectively convicting suspects, digital evidence collection is a necessity which cannot be effectively done without cross-border data sharing. The international community is rapidly shifting towards the enactment of legal frameworks to introduce effective mechanisms such as launching joint task forces for digital forensics collection or cross-border data sharing to combat cybercrime on a global scale (Clough, 2019).

International harmonisation efforts, particularly under the Budapest Convention on Cybercrime, have been widely examined. Successful prosecution of transnational cybercrime relies on unimpeded sharing of data and collaborative investigations. This, however, is often undermined by bureaucratic delays and conflicting national data privacy laws (Firdonsyah et al., 2023). In addition, scholars argue that investigative techniques should be complemented by strong ethical standards so that public confidence will not be lost, that no unintended data leaks occur during investigative extractions, and that the integrity of the evidence will be maintained all the way through the investigative process to the courtroom. Firdonsyah et al. (2023) elaborated on the critical role of ethical considerations while dealing with digital forensics frameworks. The authors are of the view that the strengthening of public trust will require the integration of additional digital forensic frameworks and ethical structures. In addition, public trust will require the development of digital forensics investigation tools that incorporate both technical and ethical frameworks to avoid public trust violations and improve public trust in digital forensic investigations. It has been determined that the continued disclosure of digital evidence stems from the inadequate preservation of critical forensic digital files (Garfinkel, 2010). It has become of paramount importance to capture and adequately analyse the various techniques and methods used to conduct digital forensics, if for no other reason than to develop frameworks to provide for a more comprehensive approach to digital forensic evidence.

Despite the Budapest Convention's prominence, significant gaps remain in comparative digital forensics legislation research. This research addresses these gaps by providing a comprehensive comparative analysis of digital forensics legislation across diverse

jurisdictions. Previous research has identified several critical deficiencies: -

Lack of Systematic Comparative Analysis

Existing literature focuses heavily on individual jurisdictions without systematic comparison across multiple legal systems. While some countries have robust digital forensics frameworks, i.e., the USA and the EU, others remain underdeveloped, making comparative analysis essential for identifying best practices and legislative gaps (Mohammed et al., 2019). This research systematically compares jurisdictions on common criteria including evidence collection procedures, search and seizure powers, privacy protection mechanisms, admissibility standards, chain of custody requirements, and cross-border data access procedures.

Limited Scope of Studies

Previous research predominantly examines developed nations' legal frameworks while overlooking emerging economies and developing nations' approaches. This limitation prevents a comprehensive understanding of the global digital forensics landscape. This research expands the geographic scope to include representatives from diverse regions.

Insufficient Case Law Analysis

The literature lacks comprehensive analysis of important judicial decisions that interpret and apply digital forensics legislation across different jurisdictions. This research incorporates analysis of key judicial decisions including Riley v. California (2014), Data Protection Commissioner v. Facebook Ireland Ltd. (2020) and Google Spain v. AEPD (2014), examining how courts interpret digital evidence standards, privacy rights, and cross-border data access.

Technology Law Gap

Many current frameworks, such as the Electronic Communications Privacy Act (1986), struggle to effectively address modern technologies including AI, cloud storage, IoT, and

blockchain systems. This research examines how different jurisdictions are adapting (or failing to adapt) their legal frameworks to emerging technologies.

Evolution of Digital Forensics Legislation

The modern laws that govern digital forensics have developed along the same lines as the computer technologies that have been developed and the criminal activities conducted as a result of the technology. The early legislation of the late 1970s and early 1980s, such as the 1978 Florida Computer Crimes Act and the 1986 United States Computer Fraud and Abuse Act, sought to define the illegal activities of accessing and manipulating data and records of computer systems. These early laws started the efforts to establish the rights and legal standing of digital records in the court system. During the same time, police agencies were starting to set up specialised units. These early units included the Federal Bureau of Investigation Computer Analysis and Response Team and signalled the beginning of police formal procedures to deal with computer evidence. During the late 1990s and early 2000s, policies to guide investigations were formalised. Formal protocols for maintaining the integrity of data are described in technical guides such as the Good Practice Guide for Digital Evidence, published by the Association of Chief Police Officers, and standards developed by the National Institute of Standards and Technology (Poore et al., 2013). With the rapid expansion of technology, especially with artificial intelligence and data being stored in the cloud, many of the older frameworks, such as the Electronic Communications Privacy Act of 1986, are struggling to effectively control the older communication channels they were designed for (Poore et al., 2013). Therefore, the legal frameworks will need to be more responsive to balance the capabilities of modern data processing against the protection of fundamental civil liberties. When computer crimes were in their infancy, they were largely a rehash of older crimes. Florida's Computer Crimes Act in 1978 was the first major piece of legislation making unauthorised access and modifications of data a crime. With the growing number of computer-related crimes, the U.S. and Canada were forced to create more federal laws in the 1980s, with amendments to Canada's Criminal Code in 1983,

and the U.S.'s Computer Fraud and Abuse Act in 1986 (Sellars, 2018).

These acts were the first major attempts to recognise the legal standing of digital evidence. By the late 1990's, the term "computer forensics" was evolving and would be rebranded to become "digital forensics" (Pollitt, 2010). The early establishment of specialised units, such as the FBI's Computer Analysis and Response Team, CART, in 1984, and the 1985 establishment of the UK's Metropolitan Police Computer Crime unit, was in recognition of the growing importance of digital evidence (Rakha, 2024). Additionally, the presence of police-sponsored events across the UK was an effort to transform the informal practices of the time into structured methodologies (Pollitt, 2010).

In 1998, the Association of Chief Police Officers (ACPO), in the UK published the Good Practice Guide for Digital Evidence, which served as the first document in the UK to describe the scope of digital evidence as well as set evaluation processes (Garfinkel, 2010). This guide described the necessity of preservation and compliance of digital evidence for court proceedings. During the latter part of the 1990s to the early 2000s, there emerged international bodies like IOCE and other initiatives aimed towards unification of practice across nations. These bodies were central in fostering collaboration between law enforcement agencies in different countries (Rakha, 2024).

Shifts toward more uniform standards began emerging in the field during the early 2000s. During this period, the National Institute of Standards and Technology started drafting best practice guidelines, which included protocols for collecting and analysing evidence in digital forensic investigations. With technological advancement, existing laws had to be changed to meet the challenges of new and emerging technologies. For example, there was controversy surrounding the applicability of the Electronic Communications Privacy Act (ECPA) of 1986 to contemporary means of communication, which resulted in queries being raised so that reforms could be implemented to ensure digital evidence is usable in investigations (Rakha, 2024).

AI has changed the approach to data interpretation in digital forensics. With the help of AI, advanced tools can process huge amounts of data at high speed and pinpoint things that human investigators may miss. This presents challenges concerning the use

of such findings in court as it demands changes to the law regarding evidence - especially with the increasing capability of the technology to collect data and monitor people (Rughani, 2017). Laws need to assist prosecution while safeguarding individuals by providing clear boundaries on data access and the scope of the investigation so that privacy is not violated. As digital cyber threats become more sophisticated, the need to build cybersecurity into digital forensics has become necessary (Rughani, 2017).

Comparative Analysis of Digital Forensics Legislation

Distinct legal traditions and policy priorities structure different statutory frameworks for digital forensics in legal systems internationally. In the U.S., digital forensics rests on the federal Electronic Communications Privacy Act 196 and the Computer Fraud and Abuse Act of 1986, as well as state laws. The Stored Communications Act of 1986 governs how U.S. federal forensics access stored electronic communications. Federal forensics units like the Federal Bureau of Investigation and the National Institute of Standards and Technology have their own procedures (Rughani, 2017). The clarifying Lawful Overseas Use of Data Act 2014 allows U.S. law enforcement to order service providers to provide requested data regardless of physical data location. Jurisdictions view digital forensics distinctly, and so do legal systems for culture and society in general (Rughani, 2017). The following table provides a comparative overview of key digital forensics legislation characteristics across selected jurisdictions:

Table 1: Comparative analysis of Digital Forensics Legislation across various jurisdictions

Criteria	USA	EU	South Africa	Australia	India	MENA
Legal System	Common Law	Civil Law	Mixed	Common Law	Common Law	Islamic Law
Primary Legislation	ECPA (1986), CFAA (1986), CLOUD Act (2018)	GDPR (2016), e-Evidence Reg. (2021)	Cybercrimes Act (2020)	Surveillance Devices Act, Criminal Code	IT Act (2000, 2008), CrPC	National Cybercrime Laws

Evidence Collection Authority	Law enforcement with a warrant	Law enforcement with judicial authorisation	Law enforcement under Cybercrimes Act	Law enforcement with warrant	Law enforcement with court permission	Law enforcement (varies by country)
Privacy Protection	Constitutional privacy + statutory protections	GDPR comprehensive protections	Constitutional privacy protections	Privacy Act protections	Constitutional privacy (emerging)	Varies by country
Admissibility Standard	Authentication + reliability required	EU framework standards	South African evidence law standards	Common law standards	Indian Evidence Act standards	National law standards
Chain of Custody	Detailed documentation required	Strict documentation protocols	Required under law	Forensic procedures required	Required by rules	Emerging requirements
Cross-Border Access	MLAT procedures, mutual assistance	MLAT + direct mechanisms under e-Evidence Reg.	MLAT procedures	MLAT procedures	MLAT procedures	Limited bilateral agreements
Technology Responsiveness	Adapting to AI, cloud, IoT	Proactive framework updates	Emerging frameworks	Modernizing continuously	Beginning to adapt	Early-stage development

In the European Union, the fundamental framework of Civil Law leads to the safeguarding of personal data through privacy laws. The General Data Protection Regulation establishes encumbrances on personal data and directs methods of digital evidence for European Union member states. The European Union streamlines cross-border investigations through the e-Evidence Regulation, which empowers judicial authorities within the European Union to compel service providers to furnish requested evidence. This regulation strikes a careful balance between constant statutory supervision of data protection and rapid evidence acquisition (Deibert & Rohozinski, 2010).

Australia is the only country in the Asia-Pacific with detailed legislation for cybercrime, embedded within its Criminal Code Act and Telecommunications Interception and Access Act 1979. India has integrated some aspects of electronic evidence and data governance into its Information Technology framework through a

combination of IT Acts and other recent digitised data protection laws (Rughani, 2017). Although these Acts and laws have gaps and limitations associated with advanced and emerging technologies, India continues to make the necessary reforms. Cybercrime laws in the MENA region have also been developed with support from the UN Office on Drugs and Crime (Gudgel, 2013). However, many countries in these regions continue to develop the systems and infrastructure to deal with digital evidence. In South Africa, the Cybercrimes Act 2020 creates a formal and systematic structure for cybercrime and the control and regulation of the power of the State to electronically seize evidence. Different regions have developed systems to deal with digital evidence and cybercrime based on their unique approaches. This overview looks at the USA, the European Union, the Asia Pacific, and the MENA regions and analyses the societal and cultural influences on the legislation with emphasis on variations and similarities (Deibert & Rohozinski, 2010).

United States

In the USA, electronic forensics is the fingerprint of State laws, and in some instances, federal laws, such as the Electronic Communications Privacy Act (ECPA) and the Computer Fraud and Abuse Act (CFAA) of 1986. While the ECPA regulates State access to electronic communications, the CFAA establishes the definitions and sanctions for unauthorised access to computer systems. These two Acts provide the essential framework for the prosecution of cybercrime that is becoming increasingly necessary. Various State Agencies, including the FBI and NIST, provide substantive and procedural measures and structures for the effective conduct of a digital forensic investigation (Gudgel, 2013).

European Union

The European Union has also made attempts to create a more cohesive legal system governing digital forensics with the General Data Protection Regulation (GDPR) as well as the eEvidence Regulation. The GDPR focuses on data protection and privacy rights, which changes the manner in which digital evidence is obtained and utilised (Ahmed et al., 2026b). Set to go into effect in March 2026, the eEvidence Regulation will facilitate the use of digital evidence exchange between EU member countries for border

investigations. This new regulation is a reminder that the member states are increasingly acknowledging that there is a need for help when it comes to cybercrime (Goddard, 2017).

Asia-Pacific Region

The digital forensics laws differ from one country to another in the Asia-Pacific region. For instance, Australia has very well-developed laws pertaining to cybercrime in the Criminal Code Act 1948 and the Telecommunications (Interception and Access) Act 1979. Meanwhile, India is still working on legal structures that support digital forensics. One of the most recent efforts is the known Indian Information Technology (Amendment) Act 2008, which tackles data protection issues as well as electronic evidence, but it also needs lots of development to be in sync with modern technology (Mishra et al., 2022).

Middle East and North Africa

In the MENA region, countries are making strides to create laws for digital forensic investigation, but they are often folded underneath existing legal frameworks aimed at governing cybercrime (Mishra et al., 2022). Countries like Tunisia are creating laws for cybercrime and digital evidence as a result of support from international bodies, such as the United Nations Office on Drugs and Crime (UNODC). That said, many countries in the MENA still lack sufficient capacity building and technical know-how to implement digital forensics (Lukonga, 2018).

Similarities and Differences in Approaches

A thorough comparison shows how different jurisdictions deal with digital forensics legislation, as there are some parallels and divergences.

Most jurisdictions understand and appreciate the balance between the protection of personal rights and the need to conduct a proper investigation. Most countries appear to have a good grasp of privacy issues, as they require warrants or legal permission to retrieve digital evidence.

However, there are large gaps in the degree of detail and comprehensiveness of the laws. The US is an outlier in this description because it has the specific law that governs electronic

communications, which is the ECPA. The rest of the world does not have those laws and relies on wider criminal codes, which often bypass and do not cater to the specific obstacles presented by digital evidence.

Impact of Cultural and Societal Factors on Legislation

Security, privacy, and technology all have one common attribute, which is culture. As a result, they have a direct impact on how legislation is constructed and followed. For example, public feeling towards privacy prevents some European countries from allowing organisations to use their data as freely as in other countries (Lukonga, 2018). We also find cultural and social factors complex in how digital forensics law is made and used. There are countries that are very protective of people's privacy, such as those in Europe, where greater emphasis is placed on laws that protect the use of people's information. This attitude would result in more stringent regulation, which would impede law enforcement in the collection of electronic traces of evidence (Saguy & Stuart, 2008).

Public or societal faith in law enforcement agencies has the ability to determine legislation. In jurisdictions where there is a 'big brother' feeling of pessimism about government power, politicians tend to be more guarded in enacting sweeping laws that make it easy to surveil citizens, potentially infringing on freedoms (Saguy & Stuart, 2008). What level of technology society has adopted also determines the way legislation is put in place (Ahmed, 2026a). Countries that have acceptable levels of technology infrastructure might be able to pass more advanced laws dealing with new technologies such as AI or the use of blockchain technology, unlike countries that are still dealing with basic cybersecurity challenges (Varner & Varner, 2014).

Key Challenges in Digital Forensics Legislation

Even though modern law enforcement and legal processes rely on digital forensics, the collection, analysis, and presentation of digital evidence pose various complications. Such issues include privacy rights, admissibility of evidence, the chain of custody, and international cooperation (Varner & Varner, 2014). This note discusses these issues in depth. One privacy concern that stands out

is the invasion of an individual's privacy that a thorough investigation entails. Digital devices contain a lot of data, which raises a number of privacy issues. To obtain relevant evidence, investigators need to access personal information, which intrudes on people's rights to privacy. Legal statutes should make sure that data collection performed during an investigation is kept to the minimum level required and within the boundaries of existing privacy regulations (Baig et al., 2017).

The introduction of the General Data Protection Regulation and similar European Union legislation has set new standards in restrictive data protection legislation. These new frameworks make demands on the collection, processing, and storage of personal data that create barriers for law enforcement in their efforts to obtain digital evidence without contravening the right to privacy (Ahmed, 2026a). In balancing privacy and the legitimate needs of society for law and order, privacy legislation has to be constantly updated in step with new technology. Evidence in its digital form raises more significant concerns than evidence in its physical form regarding its manipulation and the ease with which its integrity can be compromised. Elucidation of the particular circumstances surrounding the collection and processing of digital evidence may provide the assurance courts require for the admissibility of the evidence (Underwood, 2019).

The digital evidence must be protected by a strong chain of custody, but this is often difficult due to the rapid technological change and differing standards in various regions (Baig et al., 2017). There is a need to provide legal frameworks that outline the policies to be followed for acquiring and submitting digital evidence to the court. Maintaining the chain of custody is highly pertinent for the goal of ensuring that digital evidence is not tampered with from the time it is gathered until it is submitted in court (Granja & Rafael, 2017).

Nonetheless, the nature of the data that is classified as digital poses a challenge. The evidential value of an item of digital information is typically very volatile due to its ability to be altered and copied, castigating it's credibility when presented in court. Furthermore, the involvement of numerous agencies such as law enforcement, forensic practitioners, and lawyers tends to cloud the chain of custody even more (Novak, 2019).

Mutual Legal Assistance Treaties (MLATs)

MLATs, or Mutual Legal Assistance Treaties, are international agreements between nations that detail how requests and assistance in cases of criminal investigations are exchanged. While these treaties are vital in enabling cross-border access to digital evidence, MLATs are often very complex, slow, and cumbersome because of red tape. INTERPOL is an example of an organisation that facilitates coordination efforts by providing information and assistance to law enforcement agencies worldwide in the fight against cybercrime. These networks improve interactions and assist in the communication of crucial information related to ongoing investigations (Cortes, 2015).

Best Practices for Cross-Border Investigations

There is a need to adopt best practices aimed at improving cooperation in international digital forensics. Establishing borders for collecting digital evidence can aid in reducing differences between national legal systems and provide efficiencies in MLATs. Offering training seminars dealing with international legislation and its practical application can enhance the effectiveness of law enforcement personnel in conducting thorough investigations across borders (Firdonsyah et al., 2023).

Importance of Mutual Legal Assistance Treaties (MLATs)

Mutual Legal Assistance Treaties are the primary traditional framework for international cooperation on criminal matters. They provide a formal legal framework for requests to foreign states for electronic evidence subject to a guarantee of dual criminality and respect for the rights of the individual. Because of the nature of cybercrime, particularly the involvement of foreign servers, it may be the case that domestic law enforcement is unable to collect the remote data without committing a violation of the sovereignty of the foreign state. Treaties like MLATs greatly aid international collaboration relating to the investigation of crimes, especially for matters involving digital forensic examination (Cortes, 2015). They are treaties with a set framework between two or more states that detail the processes of aid requisition and provision regarding evidence, information, and even criminal acts. Evidence cannot be

obtained by local law enforcement agencies from outside jurisdictions that are beyond a country's borders. This is especially true for cybercrime, where computer data such as photographs, audio materials, and records are kept in foreign servers (Cortes, 2015).

MLATs facilitate providing assistance by giving a systematic model, which makes it possible to request aid in a manner that simplifies the entire process of gathering evidence from different jurisdictions. Such certainty can increase efficiency in investigations and limit the time lost during these probes. Through clarity of MLATs, countries are provided guidelines that give legal assurance both to the requesting and requested states. In addition, it helps in making sure that requests are handled legally, and the rights of people are protected during investigations (Bisset, 2023). Within the confines of the traditional treaties, although they are often characterised by their slow and inefficient bureaucratic processes, an increase in trust and communication within law enforcement agencies exists due to their collaborative nature. The rapid evolution of technology, in which the integrity of digital evidence is at risk, has been a critical factor in the traditional treaties' processes being frequently characterised by a lack of timeliness (Cortes, 2015).

Such collaboration is crucial for the effective management of transnational crime due to the nature of cybercriminals operating in many jurisdictions. MLATs can aid in building capability by fostering the sharing of information and good practices among signatories, which enables them to better fight cybercrime. On the other hand, there are several other challenges that include bureaucratic slowdowns and a lack of enthusiasm by other countries to actually do the requested actions. For instance, countries without MLATs may have a more difficult time obtaining vital information from foreign service providers, which is the case with Pakistan not being able to receive cybercrime data from the United States because of MLATs (Pullen, 2019).

Analysis of the Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime provides a comprehensive framework for unifying substantive cybercrime definitions, procedural powers, and international cooperation mechanisms. It establishes standardised offences, including illegal

access, system interference, and computer fraud, while equipping member states with procedural tools such as expedited data preservation, production orders, and search authorisations for computer data.

Like other strategies, this one aims to delineate a legal definition of cyber offences, including illegal access to systems and data, data and system interference, and other forms of computer-based fraud. The convention aids in the prosecution of international cybercriminals by establishing a minimum threshold common to all parties to the convention (Karagiannis & Vergidis, 2021). This defines the procedural powers needed to combat cybercrime and collect electronic evidence. These include the quick acquisition of information, the storage and retrieval capabilities of IT systems, and the interception of communications (Ahmed et. al, 2025). The treaty has greatly impacted international cybercrime laws, as many states that are not parties to the treaty have utilised it as a blueprint for reforming their national laws. The treaty is a part of the Cybercrime Convention Committee, which aids in the enhancement of capabilities and the modernisation of procedural means (Ahmed, 2026a). The adoption of additional protocols for advanced access to the cloud and direct interaction with service providers is an effort to revise and improve the Convention. By providing common legal definitions and procedural standards, the treaty enhances the interoperability of digital forensic investigations across borders (Karagiannis & Vergidis, 2021).

The Budapest Convention reiterates the need to achieve international collaboration through the provision of mutual legal assistance to member countries, including the exchange of information and coordination of actions in criminal investigations (Cortes, 2015). The Convention has been supported by capacity-building projects undertaken by the Cybercrime Convention Committee (T-CY) and global programs aimed at strengthening national capacities for the investigation and prosecution of cybercrime (Nguyen & Golman, 2020).

International forensics specialists have to cooperate to deal efficiently with digital forensics legislation issues around the globe, which is greatly influenced by the Budapest Convention. They need only look at the principles carved by the Budapest Convention, and most developed legislation emerges in consideration of cybercrime and other digital evidence. It has been reported that around 177

states, and counting, between 2018 and 2020, are reforming their laws in the path in accordance with this treaty's guidelines (Nguyen & Golman, 2020). The procedural powers defined by the convention have improved the ability of law enforcement to obtain electronic evidence in a more effective manner. The forensic practitioners' communities of states that have adopted these powers are better prepared to deal with more sophisticated cases of cybercrime with a digital forensic component. The convention facilitates cooperation among practitioners from different countries in order to learn from each other's experiences and best practices for the performance of digital forensics investigations. This, in turn, makes the entire capability to combat cybercrime much better (Clough, 2019).

Case Law Analysis

This section examines important legal decisions that interpret and apply digital forensics legislation across jurisdictions:

United States

In the case of (Riley v. California, 2014), it was established that mobile devices require an independent warrant for searches, recognising the vast storage capacity and personal nature of modern smartphones. Furthermore, in the case of (United States v. Apple, 2024), the Court addressed encryption and government access to digital evidence, exploring the tensions between law enforcement access and privacy protection. Furthermore, it was held that government access to cell-site location information requires a warrant, establishing privacy protections for digital location data.

European Union and Member States

In the case of Google Spain SL v. AEPD (2014), the Court established the right to be forgotten, affecting digital evidence preservation and personal data in digital investigations. Furthermore, in the case of *Data Protection Commissioner v. Facebook Ireland Ltd. (2020)*, the Court addressed the adequacy of data transfer mechanisms between the EU and third countries, with implications for international digital evidence sharing. Lastly, concerning the Google case of 2017, the Court clarified the digital privacy protections regarding cookies and digital tracking.

South Africa

In the case of Bernstein v. Bester (1996), the court established constitutional protection of privacy as foundational to digital evidence cases. Furthermore, emerging jurisprudence under the Cybercrimes Act (2020) continues to develop standards for digital evidence admissibility and investigation procedures.

Ethical Considerations in Digital Forensics

Legal and ethical parameters must be qualified and quantified to maximise the effectiveness of digital forensic laws, particularly in the case of law enforcement agencies which have to ensure minimal infringement on civil liberties while fulfilling their operational mandates. This is even more complex during the retrieval of personal information and data (Broadhurst, 2006). Ethical boundaries should help legal practitioners in these dilemmas while giving guidelines on how to stay within the law. Ethically, there must be a consideration of the right to privacy, restricted data gathering, and openness on how the check was done to gather information (Broadhurst, 2006). Maintaining the integrity of digital forensic investigations in the judicial system is reliant on an ethical framework. Practising forensic professionals must have an ethical framework regarding the minimisation of data and the preservation of unnecessary personal information that is collected during the forensic examinations of devices, from being exposed or compromised. Jurisdictions must have an ethical framework regarding the transparency of forensic investigations and the validation of the techniques and tools, and the errors that may be present. There must be an ethical framework to address the concerns of digital forensic practitioners.

These guidelines should provide steps to take to protect sensitive personal information when it is captured during investigations.

Digital evidence must be collected and analysed in an open manner, where practitioners' involvement, methods, and processes should be transparent.

Studying ethics provisions in case studies of digital forensics will help understand some of the most contemporary issues practitioners have to work with. These case studies demonstrate how

ethical issues have to be accounted for within the investigative processes and also in policy formation (Stoyanova et al., 2020).

Equipping personnel involved in digital forensics investigations requires investing in training initiatives. Modern investigators must learn new technologies, laws, and procedures through Continuing Education Promotion legislation (Stoyanova et al., 2020). Training should encompass both technical components of forensic communication and soft components, including skilful communication and ethical decision-making. Comprehensive professional training is necessary to equip forensic investigators, prosecutors, and judges with both technical knowledge and ethical decision-making skills (Ahmed et al., 2025). There must be fruitful collaborations between universities and law enforcement to form ethical frameworks and standardised methods to develop curricula for digital investigations that respect the rights of citizens. An integrated approach that is constructive in nature will impact the frameworks for teaching digital forensics. The goal of such partnerships between universities is to create a highly qualified workforce that is able to respond to a diverse array of challenges (Firdonsyah et al., 2023). Educational institutions and other stakeholders need to conduct capacity building to better understand newer, emerging forms of cybercrime and develop new educational curricula targeting law enforcement agencies. A collaboration between education and law enforcement amplifies the outreach of innovations and the implementation of solutions in the field (AlDaajeeh et al., 2022).

Suggestions and Recommendations

Digital technologies impact every aspect of criminal activity, and the flexibility of digital legislation and digital criminal investigations is an imperative. With the complexity of cybercrime, legislation in every jurisdiction seeks to find a balance between providing solutions and not infringing on civil liberties and the right to privacy. To address the hurdles in the internationally accepted principles of digital forensics, parliaments should adopt a limited scope of legislation on the admissibility of digital evidence. Legislation should clearly describe the procedures for the extraction of data from digital devices, the documentation of the chain of custody, and the verification of the integrity of data. Harmonisation

of these procedures will eliminate legal differences and promote the acceptance of digital evidence in cross-border legal proceedings. States should create expedited, non-content-direct-request frameworks using modern cross-border legal frameworks. By creating a framework allowing law enforcement to send direct legal orders to Internet service providers, considerable time delays from traditional diplomacy are removed, and the request is still legally validated. Parliaments should also modify evidentiary frameworks to include the use of artificial intelligence in digital forensics. Digital forensics, including automated software, must also meet the judicial standard of reliability. To achieve this, software must comply with standards of peer review and be transparent with the code. Establishing statutory requirements for algorithmic validation will ensure that artificial intelligence findings can withstand legal scrutiny in court. In light of the above discussion, the following suggestions and recommendations have been offered with an aim to fulfil the research objective of diversifying the international outlook in the realm of digital forensics legislation.

Harmonisation of Legal Frameworks

There is a dire need to unify laws which govern digital forensics and for which countries are required to take steps to introduce domestic legislation arising out of prospective international treaties. International Organisation for Standardisation (ISO) and the International Telecommunication Union (ITU) can play a pivotal role in the process of collaboration and harmonisation by helping countries develop procedures pertaining to the preservation, collection and analysis of digital forensic evidence. This can ensure that forensic procedures are synchronised among states, which will increase the likelihood of accepting evidence in international legal forums. It is, therefore, imperative to draft model legislation which states could rely upon and either deploy the same or modify it to fit their particular jurisprudential landscape. This draft legislation should aim to address such important concepts as digital evidence, its collection, preservation, and admissibility at different legal forums.

Training and Capacity Building

There is a need to deploy more resources into the training of law enforcement professionals, judiciary members, and forensic specialists to enable them to correctly analyse digital evidence and to enhance the processes involved in conducting digital forensics. This can be achieved through creating training modules which incorporates advanced technological standards, legal standards, and ethical standards which are required to be adopted in digital forensics by the field professionals. This training should be made mandatory for all employees who are involved in the process of handling and managing digital evidence. Furthermore, there is a need to encourage collaboration between law enforcement agencies and academia for the creation of specialised courses and workshops which respond to new developments in cybercrime and the effective handling of digital forensics evidence.

Strengthening Privacy Protections

It is equally important to enhance privacy protection mechanisms for personal data alongside digital forensics legislation so that impartial, fair and effective digital forensics investigations can be conducted. A privacy impact assessment should be conducted prior to the application of new digital forensic technologies or practices so that their consequences on privacy could be assessed beforehand. This would help in mitigating various individual privacy concerns which are likely to be raised. Moreover, it is equally crucial to set out specific legal parameters which control the requisite personal data access during digital forensics investigations for the use of such data.

Addressing Emerging Technologies

With the rapid change in technology, the law must follow the same pace. Therefore, new legislation and a revised legal landscape are *sine qua non* for effectively addressing as well as regulating emerging technologies such as AI, blockchain technology, and cloud computing. There is a need to formulate effective guidelines which specifically address the threats posed by new technologies. For instance, prospective legislation should specify what happens when AI-driven evidence is presented before

a legal forum and how its credibility should be determined, what the standard of proof would be, and on whom the onus of proof lie while presenting digital or AI-driven evidence. Questions such as these demand effective prospective legislation so that they could be appropriately addressed.

Promoting Ethical Standards

There is a need to promote ethical standards and a strict requirement to follow them while conducting digital forensics investigations, as well as when handling digital evidence. This would help establish the norms of professionalism and integrity within the institutional framework so that the impartiality and credibility of such investigations and digital evidence could not be called into question at any legal forum. Therefore, it is necessary that an ethical review board should also be established to evaluate whether the ethical standards were adhered to by the investigators and law enforcement professionals when conducting digital forensics investigations or when handling or collecting digital evidence.

The above-given recommendations are intended to modify and evolve the digital forensics landscape on an international scale with the intention of creating a progressive approach towards this domain which is development oriented, socially acceptable, and ethically appropriate in nature. States can better prepare to combat cybercrime in a rights-respecting manner through effectively standardising legal systems, improving institutional structures, enhancing privacy regulations, setting accreditation criteria, and addressing new technologies. Through coordinated action at the state level and cooperation with other nations, it is possible to create a safer cyberspace that serves justice while protecting the basic structures of a democratic society.

Conclusion

Within only a few decades, the change in technology has actually changed the outcome of criminal investigations for the better, especially in the forensic field. There is a dire need for legislation to be adaptable and responsive to the growing sophistication of cybercrime in digital forensics. The focus of this

research paper has been on different approaches to international law and digital forensics, especially on the peculiarities of the legal constructs, barriers, and the most effective solutions in different places. These conclusions point to the clear gap that exists between the needs for fighting cybercrime whilst respecting people's liberties through well-coordinated international relations. One of the deeper observations from this research is how different countries have different legislation relating to digital forensics. In certain areas, there are well-developed laws that consider digital evidence, while in others there are jurisdictions with laws that are rather obsolete and unsuitable. This situation decreases the efficacy of how borderless investigations are conducted, and cybercriminals tend to take advantage of this fact. Therefore, there is a dire need to make efforts towards a unified legal framework which could potentially harmonise the countries' approach towards digital forensics investigation and digital evidence handling so that international and domestic disputes pertaining to these domains could be sufficiently addressed.

This research has made a novice attempt to identify the major obstacles and dilemmas which law enforcement agencies and legal practitioners face when they are conducting digital forensics investigations or when handling digital evidence. For instance, privacy rights, data protection, and admissibility of digital evidence are some of the many considerations that are still problematic to this day. Furthermore, it is impossible to ignore the impact of emerging technologies on digital forensics investigations and digital evidence. The increasing usage and development of AI and cloud computing, along with blockchain technology, have led to the creation of novel challenges pertaining to the collection and analysis of digital evidence and conducting digital forensics investigations. Therefore, there is a dire need for uninterrupted vigilance and prompt action to be taken by the stakeholders to tweak the present laws to cater for these changes. Ultimately, only a coherent legal framework governing digital forensics and digital evidence is the solution if one is seeking to permanently address the problems faced by the existing legal landscape.

References

Ahmed, S. S. (2026a). Cross-Border surveillance and the right to privacy: legal remedies in the age of 5G and IOT. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.6000814

Ahmed, S. S., Cheema, Q. U. A., & Fatima, S. (2026b). Bridging the Transparency Gap: A Comparative Analysis of the Right to Explanation Under the EU AI Act and the GDPR. *Pakistan Journal of Law, Analysis and Wisdom*, *5*(6), 20–38. https://pjlaw.com.pk/index.php/Journal/article/view/v5i6-20-38

Ahmed, S. S., Javed, M. S., & Haider, S. (2025). Algorithmic Discrimination and the Law: Regulating Bias in AI Decision-Making. *Pakistan Journal of Humanities and Social Sciences*, *13*(4), 220–229. https://doi.org/10.52131/pjhss.2025.v13i4.3086

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, *119*, 102754. https://doi.org/10.1016/j.cose.2022.102754

Alshumrani, A., Clarke, N., & Ghita, B. (2023). A Unified Forensics analysis approach to digital investigation. *International Conference on Cyber Warfare and Security*, *18*(1), 466–475. https://doi.org/10.34190/iccws.18.1.972

Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., Johnstone, M., Kerai, P., Ibrahim, A., Sansurooah, K., Syed, N., & Peacock, M. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*, *22*, 3–13. https://doi.org/10.1016/j.diin.2017.06.015

Beebe, N. (2009). Digital Forensic Research: the good, the bad and the Unaddressed. *IFIP Advances in Information and Communication Technology*, 17–36. https://doi.org/10.1007/978-3-642-04155-6_2

Bernstein v. Bester [1996] 2 SA 751

Bisset, A. (2023). The Mutual Legal Assistance Treaty for Core Crimes. *Nordic Journal of International Law*, *92*(2), 218–247. https://doi.org/10.1163/15718107-bja10056

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing an International Journal*, *29*(3), 408–433. https://doi.org/10.1108/13639510610684674

Casey, E. (2010). Handbook of Digital Forensics and Investigation. In *Elsevier eBooks*. https://doi.org/10.1016/c2009-0-01683-3

Casey, E. (2011). *Digital Evidence and Computer crime: Forensic science, computers and the internet*. http://ci.nii.ac.jp/ncid/BB06007590

Chung, H., Park, J., & Lee, S. (2017). Digital forensic approaches for Amazon Alexa ecosystem. *Digital Investigation*, *22*, S15–S25. https://doi.org/10.1016/j.diin.2017.06.010

Clough, J. A. (2019). A world of Difference: The Budapest Convention on Cybercrime and the Challenges of harmonisation. *Monash University Law Review*, *40*(3), 698–736. https://doi.org/10.26180/5db8050ca2b5b

Cortes, S. (2015). MLATS and TorBrowser: Mutual Legal Assistance Treaties in Online Anonymity Technology and Domestic Surveillance. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2564218

Cybercrimes Act 19 of 2020 (South Africa). https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf

Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems, Case C-311/18, ECLI:EU:C:2020:559 (Court of Justice of the European Union, July 16, 2020). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311

Deibert, R. J., & Rohozinski, R. (2010). Risking Security: Policies and paradoxes of cyberspace security. *International Political Sociology*, *4*(1), 15–32. https://doi.org/10.1111/j.1749-5687.2009.00088.x

Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986). https://uscode.house.gov/statutes/pl/99/508.pdf

Firdonsyah, A., Purwanto, P., & Riadi, I. (2023). Framework for Digital Forensic Ethical Violations: A Systematic Literature Review. *E3S Web of Conferences*, *448*, 01003. https://doi.org/10.1051/e3sconf/202344801003

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, *7*, S64–S73. https://doi.org/10.1016/j.diin.2010.05.009

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. *International Journal of Market Research*, *59*(6), 703–705. https://doi.org/10.2501/ijmr-2017-050

Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, ECLI:EU:C:2014:317 (Court of Justice of the European Union, May 13, 2014)

Granja, F. M., & Rafael, G. D. R. (2017). The preservation of digital evidence and its admissibility in the court. *International Journal of Electronic Security and Digital Forensics*, *9*(1), 1. https://doi.org/10.1504/ijesdf.2017.081749

Gudgel, J. (2013). Internet Privacy Policy Paradoxes: The Electronic Communications Privacy Act (ECPA) Amendments Act of 2013 & the Consumer Privacy Bill of Rights of 2012. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2257647

Karagiannis, C., & Vergidis, K. (2021). Digital Evidence and Cloud Forensics: contemporary legal challenges and the Power of Disposal. *Information*, *12*(5), 181. https://doi.org/10.3390/info12050181

Klasén, L., Fock, N., & Forchheimer, R. (2024). The invisible evidence: Digital forensics as key to solving crimes in the digital age**.** *Forensic Science International*, *362*, Article 112133. https://doi.org/10.1016/j.forsciint.2024.112133 .

Lukonga, I. (2018). Fintech, Inclusive Growth and Cyber Risks: focus on the MENAP and CCA regions. *IMF Working*

Paper, *18*(201), 1. https://doi.org/10.5089/9781484374900.001

Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security*, *120*, 102820. https://doi.org/10.1016/j.cose.2022.102820

Mohammed, K. H., Mohammed, Y. D., & Solanke, A. A. (2019). Cybercrime and Digital Forensics: Bridging the Gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria. *International Journal of Cybersecurity Intelligence and Cybercrime*, *2*(1), 56–63. https://doi.org/10.52306/02010519zjrk2912

Mouhtaropoulos, A., Li, C.-T., & Grobler, M. (2014). Digital forensics: A regional comparison of clinical and educational requirements. *Journal of Digital Forensics, Security and Law*, *9*(2), 143–158. https://doi.org/10.52306/02010519ZJRK2912

Nguyen, C. L., & Golman, W. (2020). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action.' *Computer Law & Security Review*, *40*, 105521. https://doi.org/10.1016/j.clsr.2020.105521

Novak, M. (2019). Digital evidence in criminal cases before the U.S. Courts of Appeal: Trends and issues for consideration. The Journal of Digital Forensics, Security and Law. https://doi.org/10.15394/jdfsl.2019.1609

Pollitt, M. (2010). A history of digital forensics. In *IFIP advances in information and communication technology* (pp. 3–15). https://doi.org/10.1007/978-3-642-15506-2_1

Poore, J., Flores, J. C., & Atkison, T. (2013). Evolution of digital forensics in virtualization by using virtual machine introspection. *ACM Digital Library*, 1–6. https://doi.org/10.1145/2498328.2500078

Pullen, P. J. (2019). Nail in the MLAT coffin: Examining Alternative solutions to the current Mutual Legal Assistance Treaty Regime in International Cross-Border Data Sharing.

North Carolina Journal of International Law, *44*(4), 1. https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=2064&context=ncilj

Rakha, N. A. (2024). Cybercrime and the Law: Addressing the challenges of digital forensics in criminal investigations. *Mexican Law Review*, 23–54. https://doi.org/10.22201/iij.24485306e.2024.2.18892

Riley v. California, 573 U.S. 373 (2014).

Rughani, P. H. (2017). ARTIFICIAL INTELLIGENCE-BASED DIGITAL FORENSICS FRAMEWORK. *International Journal of Advanced Research in Computer Science*, *8*(8), 10–14. https://doi.org/10.26483/ijarcs.v8i8.4571

Saguy, A. C., & Stuart, F. (2008). Culture and Law: Beyond a paradigm of cause and effect. *The Annals of the American Academy of Political and Social Science*, *619*(1), 149–164. https://doi.org/10.1177/0002716208320458

Sellars, A. (2018). Twenty years of web Scraping and the Computer Fraud and Abuse Act. *SSRN Electronic Journal*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3221625

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, *22*(2), 1191–1221. https://doi.org/10.1109/comst.2019.2962586

Underwood, T. (2019). *Distant Horizons: digital evidence and literary change*. https://experts.illinois.edu/en/publications/distant-horizons-digital-evidence-and-literary-change

United States v. Apple Inc., No. 2:24-cv-04055 (D.N.J. Mar. 21, 2024).

Varner, I. I., & Varner, K. (2014). *The relationship between culture and legal systems and the impact on intercultural business communication*. DigitalCommons@EMU. https://commons.emich.edu/gabc/vol3/iss1/3/?utm_source=commons.emich.edu%2Fgabc%2Fvol3%2Fiss1%2F3&utm_medium=PDF&utm_campaign=PDFCoverPages