Digital Evidence in Foreign Jurisdiction and Quality of Justice

Bayazid Hossain*

Abstract
In an increasingly interconnected digital world, the concept of the right and access to digital evidence from a foreign jurisdiction has emerged as a fundamental human rights issue in the globe. This right asserts that individuals and/or States should have the right to access information stored beyond their national borders, reflecting the globalized nature of data storage and its profound implications for ensuring justice in true sense universally. This article explores the legal framework and associated challenges of the right to online evidence under international law. International human rights instruments, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, provide a foundation for its recognition. However, the extraterritorial nature of online information storage and States' reluctance question the quality of justice globally resulting in a complex landscape. On top of that the challenges associated with this right include conflicts of jurisdictions, issues of state sovereignty, and the extraterritorial application of domestic laws. Case studies involving cross-border data access also illustrate the complexities involved. Furthermore, the paper discusses the potential discriminatory consequences of this asymmetry, as jurisdictions with greater access to online evidence may enjoy a distinct advantage in legal proceedings involving foreign parties. This raises questions about the fairness and impartiality of the global legal system and underscores the need for international cooperation and equitable frameworks for evidence sharing.

Key-words: Evidence, digital jurisprudence, RTI, jurisdiction and human rights.

1. Introduction
In today’s interconnected world, the rapid proliferation of digital technologies has brought forth unprecedented opportunities for communication, collaboration, and innovation. Digital evidence has been a fundamental requirement globally.\(^1\) It has increased the potentials of judicial activism and aspirations towards the true meaning of justice in accusatorial justice system. The quality of justice provided in the digital age has in many cases received the privileges of digital evidence support

\(^*\) Assistant Professor of Law, Bangladesh Open University, Bangladesh, E-mail: bayazidh7@gmail.com.

\(^1\) Corey S. Shdaimah, Michael W. Yarbrough, Steven A. Boulanger, Research Handbook on Law, Movements and Social Change (Edward Elgar 2023) 7.
from both national and international agencies. This experience is global and Bangladesh is also an illustration for having digital evidence support from facebook. However, such privileges have not been fostered as a right although it ought to be. This digital age has also given rise to complex challenges, chief among them being the critical need for safeguarding digital security and protecting individuals’ rights to privacy. In this dynamic landscape, the concept of transnational Right to Information (RTI) emerges as a pivotal framework that not only addresses these challenges but also seeks to bridge the gap between theories and practices in digital security across diverse global contexts.

The United States, often considered a vanguard in digital innovation, and the Global South, representing a multitude of nations with distinct socio-economic and political landscapes, stand at the forefront of this evolving discourse. This context sets the stage for a comprehensive exploration of the theories and practices surrounding online evidence in custody of foreign jurisdiction for Digital Security. In this regard, the cross-border right to information available in online framework recognizes that the flow of digital information knows no boundaries, making it imperative to view digital security through a global lens. It emphasizes that individuals should have the right to access information about data collection, surveillance, and other digital practices that impact their lives, regardless of their geographic location. Moreover, it underscores the importance of individuals in the technologically unprivileged countries who often find themselves at the intersection of digital innovation and vulnerabilities, and their role in shaping global conversations on digital security.

Trials are nowadays treated as smart justice for using smart evidencing. In order to conduct a successful investigation, it is important to gather digital evidence that has been protected and confirmed by cybersecurity professionals. Until they can verify the digital evidence they have obtained, pertinent cybersecurity specialists should exercise caution while speaking with the media and the broader public. This research will study the extent of smartness of courts of both technologically privileged and dependent States in delivering justice.

This paper will explore three basic questions. Firstly, what are the cultural and societal factors that shape the attitudes and behaviors of individuals, organizations, and governments towards transnational RTI as a right to evidence leading to right to justice in true sense? Secondly, what are the common practices and challenges associated with the exercise of RTI in the digital security domain in the United States and Global South? Thirdly, how does the implementation of the right to online evidence in the context of digital security impact on the quality of justice?

---


2. Research Approach

This study will conduct an extensive literature review to gain a comprehensive understanding of the theoretical frameworks, legal provisions, and existing research related to online evidence digital security in both the United States and global south countries, especially Bangladesh. A diverse set of case study countries from the Global South will be selected in order to investigate how transnational RTI is applied in different cultural, political, and technological contexts. These case studies are intended to encompass a mix of high and low-income countries to capture a wide range of experiences. This article will analyze relevant documents, reports, legal texts, and online content to identify trends, challenges, and best practices related to right to digital evidence for justice. On top of that, a comparative approach will be in this to examine the differences and similarities in the implementation of the effective access to online evidence between the tech-giant States and developing countries. Employment of thematic analysis to identify key themes and patterns emerging from the available data from relevant primary and secondary sources will play a significant role. This qualitative research approach will enable a deeper understanding of how right to online evidence is applied in different contexts and contribute to the broader discussions on digital security, transparency, and accountability in the digital age.

3. Research Limitation

The research will have some specific areas. It will not include all forms of digital evidence and only the private communications in course of social media platforms applications required by courts are the subjects of this study. The impact assessment of overseas of digital evidence in custody of overseas authorities will be studied within the US and Bangladesh. Within the meaning of right to information, this paper deals with right to information for judicial purposes only. There is argumentative limitation in this paper. This research does not argue that technologically developed States should sacrifice their social values and State interest in providing personal data to be used as evidence in a non-US court. It however advocates for ensuring an effective mechanism to provide evidence from US platforms to be required in non-US courts where parties are also the nationals of requesting country or the parties voluntarily are seeking justice even either of them is not the citizen of that country.

4. What Makes ‘Online Evidence’ in Digital Platforms?

Online evidence, also referred to as digital evidence or electronic evidence, is a term used to describe information and data collected from digital sources on the internet or electronic devices. Any admissible material that is recorded in binary form or sent in digital form and that a party to a lawsuit may use at trial is considered to be ‘digital evidence,’ sometimes known as ‘electronic evidence.’

4 ‘COLLECTION OF DIGITAL EVIDENCE’, (September, 2023), available at: <https://public.power
mails, digital photos, ATM transaction logs, word processing documents, instant message histories, spreadsheets, internet browser histories, databases, the contents of computer memory, computer backups, computer printouts, GPS tracks, logs from a hotel’s electronic door locks, and digital video or audio files are just a few examples of digital evidence.

There is no universally agreed-upon definition from specific scholars. Fredric I. Lederer defines digital evidence as ‘evidence in the form of electronic data that is stored on, generated by, or transmitted via an electronic device or computer system. This evidence may include text, images, audio, video, or other types of digital information.’ They represent the combination of numbers in texts, audio or video any other electronic version relevant to specific cases in courts. One thing is common i.e. this type of evidence is created online and its verification requires access.

Online evidence always emphasizes the digital nature of online evidence and its relevance in legal disputes. Online evidence can encompass a wide array of information, including emails, social media posts, chat logs, digital documents, metadata, and more. Its significance lies in its potential to support or refute claims in various legal contexts, including criminal investigations, civil litigation, and regulatory matters.

5. Why Rights to Evidence are Human Rights?

The philosophy of the right to evidence is a fundamental concept within the realm of legal philosophy and jurisprudence. It centers on the idea that individuals involved in legal proceedings have a fundamental right to access and present evidence in their favor to ensure a fair and just outcome. This philosophy is essential for upholding principles of due process, fairness, and the rule of law in legal systems around the world.

Due process, fairness and presumption of innocence are three basic elements of adversarial jurisprudence. The right to evidence is closely linked to the concept of due process, a fundamental principle in legal philosophy. Due process requires that individuals have a fair and impartial opportunity to be heard and to present their case. This includes the right to access and introduce evidence that is relevant to their defense. The US Supreme Court held that prosecutors are obligated to disclose exculpatory evidence to the defense, emphasizing the importance of fairness in the criminal justice system. The right to evidence aligns with the presumption of innocence, another cornerstone of justice systems. The accused is

---

presumed innocent until proven guilty, and access to evidence is crucial for individuals to challenge the prosecution’s case and establish their innocence. This principle is enshrined in legal systems worldwide. Many legal systems, including the common law tradition, operate on an adversarial model, where the parties involved actively present evidence and arguments to an impartial decision-maker. This system relies on the right to evidence to ensure that each side has an equal opportunity to make their case. The right to evidence is a fundamental aspect of the adversarial system.

Rights to evidence are also indisputably recognized as human rights. International human rights instruments, such as the Universal Declaration of Human Rights\(^9\) and the International Covenant on Civil and Political Rights\(^10\), emphasize the right to a fair trial, which includes the right to present evidence and have access to evidence that is relevant to the case. These documents reflect the global recognition of the importance of the right to evidence.

The safeguard of the accused balancing interests are also pertinent in the philosophy of rights to evidence. In some legal systems, there is a principle known as the exclusionary rule, which prohibits the use of evidence that has been obtained in violation of the accused’s rights. The case in the United States established the exclusionary rule for illegally obtained evidence, further emphasizing the importance of respecting the right to evidence.\(^11\) While the right to evidence is fundamental, it is not absolute. Courts often engage in a balancing act between the right to evidence and other important interests, such as national security or the protection of confidential information. This is evident in cases like United States v. Reynolds, where the government’s interest in national security was weighed against the right to evidence.\(^12\)

It is, therefore, undeniable that the philosophy of the right to evidence emphasizes the critical role that evidence plays in legal proceedings and its significance in upholding principles of fairness, due process, and the rule of law. It is a foundational concept that is enshrined in legal systems, international human rights instruments, and legal precedents worldwide, ensuring that individuals have the opportunity to present their case and challenge the evidence against them in a just and equitable manner.

In today’s interconnected world, the digital landscape transcends geographical boundaries, and information flows seamlessly across borders. As a result, questions about the rights of individuals to access information that is stored beyond their own national borders have become increasingly relevant. The concept of the access to digital evidence in overseas authority as of rights emerges as a pivotal issue at the intersection of technology, human rights, and jurisdictional boundaries. This

---

right, which asserts that individuals should have the ability to access information stored abroad, has profound implications for the protection and realization of human rights in the digital age.

The right to online evidence from extra-territorial custody encompasses a range of vital human rights principles, including the right to freedom of expression, the right to privacy, and the right to access information. It is a response to the globalized nature of information storage and the increasing reliance on digital platforms for communication, commerce, and the exercise of fundamental rights. As individuals and entities increasingly store their data and information in data centers and servers located in foreign jurisdictions, questions about the reach of national laws, the protection of user rights, and the ability to seek redress in cases of infringement have come to the forefront of international human rights discussions. This right is not only a matter of convenience or technological necessity but a fundamental human rights issue that implicates the ability of individuals to exercise their rights and freedoms in an interconnected world. It raises crucial questions about the sovereignty of nations over data, the balance between national security and individual rights, and the role of international human rights instruments in addressing the challenges posed by extraterritorial data custody.

This introduction sets the stage for a deeper exploration of the Right to Online Information from Extra-territorial Custody as a human rights issue. By examining the legal, ethical, and practical dimensions of this right, we can gain insights into the evolving landscape of human rights in the digital age and the challenges and opportunities it presents for the protection of individual liberties, global justice, and the advancement of a rights-based approach to online information access. In the following sections, we will delve into the legal frameworks, case studies, and ethical considerations surrounding this critical issue, with the aim of shedding light on its significance in today’s interconnected and data-driven world.

6. Right to Justice with or without Digital Evidence

The concept of a cross-border right to digital evidence as a human right within the framework of existing international laws is a complex and evolving area of jurisprudence. It intersects with various fundamental human rights, including the right to privacy, the right to a fair trial, and the right to access information. A foundational issue is the tension between national sovereignty and jurisdiction in a borderless digital world. Traditional legal concepts of territorial jurisdiction may not align with the global nature of digital evidence. Theoretical discussions often revolve around the question of which country’s laws should apply when digital evidence is located across borders. The theoretical underpinning of cross-border right to digital evidence is often rooted in human rights principles. Access to evidence is a fundamental aspect of the right to a fair trial. The right to privacy
also plays a crucial role, as international law seeks to balance access to evidence with individuals’ rights to data protection and privacy. The concept of extraterritoriality comes into play when a national court seeks to compel the production of digital evidence located in another country. Theoretical debates center on the conditions under which a country’s laws can be applied beyond its borders and the principles of comity, non-interference, and respect for the sovereignty of other nations.

The International Covenant on Civil and Political Rights (ICCPR) recognizes the right to privacy. This right includes protection against arbitrary or unlawful interference with an individual’s privacy, family, home, or correspondence. Cross-border access to digital evidence should not infringe upon an individual’s right to privacy, and any such access must be lawful, necessary, and proportionate. The ICCPR also enshrines the right to a fair trial. In a digital context, this right implies that individuals should have access to digital evidence relevant to their cases. Denying access to such evidence could hinder the ability to present an effective defense, potentially violating the right to a fair trial.

Although not explicitly enshrined in a single international treaty, the right to access information is supported by various international instruments and UNESCO’s recognition of the importance of access to information as a fundamental human right. This right can extend to individuals seeking access to digital evidence held across borders, particularly in cases where such information is essential to the protection of their rights. International law recognizes the principle of state sovereignty, which gives states authority over actions that occur within their territorial boundaries. However, with digital evidence often stored outside national borders, there is an ongoing debate about the extent to which states can exercise jurisdiction and demand access to data held by foreign entities without violating the sovereignty of the host country.

While not human rights instruments, Mutual Legal Assistance Treaties (MLATs) are bilateral or multilateral agreements that facilitate the exchange of evidence and information across borders in criminal investigations. These treaties often serve as practical mechanisms for addressing cross-border access to digital evidence while respecting international legal principles. It is crucial to recognize that the rapid advancement of technology has outpaced the development of explicit international legal frameworks to address cross-border digital evidence. This has led to jurisdictional conflicts, differing national approaches, and debates over the balance between security and individual rights.

16 ibid.
7. ‘Reasonable Doubt’ in Digital Age

The doctrine of reasonable doubt in criminal cases involving digital evidence in proving or disproving any fact has been an unconventional crisis in cyber jurisprudence. The theory and practices of reasonable doubt in traditional criminal trial and the same in cyber tribunals or courts around the world are mostly similar. Burden of proving the guilt in these countries lies to the governments of South Asian countries, EU and the US. The presumption of innocence is historically given strength in a criminal trial setting principally by the need that the prosecution establishes the defendants’ guilt beyond a reasonable doubt. Obviously this is justified without digital evidence, and it remains a fundamental principle in criminal justice systems even when digital evidence is not present or is limited. However, in the age of digital communication, we cannot expect that every communication would be done offline. The conviction rate of cyber crime in Bangladesh is less than 1% whereas, the total number internet users is over 12.61 crore. Conviction is inevitable if there is no sufficient evidence to prove the connection. With this viewpoint, I am not arguing that benefit of doubt should be abolished from Bangladesh. I just argue that scenario of comparative conviction rates, internet users and scopes of using the most available online evidence offer substantial differences in the quality of justice in technologically privileged and dependant States.

8. ‘Reasonable Doubt’ in the US Courts and Digital Evidence

The doctrine of reasonable doubt is a fundamental principle in criminal law that places a heavy burden on the prosecution to prove the guilt of the accused beyond a reasonable doubt. This principle is enshrined in the legal systems of many countries, including the United States. The test gave the presumption of innocence tangible support, the United States Supreme Court expressly recognized it as legally necessary in *In re Winship* case saying that the Due Process Clause protected the accused against conviction except upon proof beyond a reasonable doubt of every fact necessary to constitute the crime charged. The rule works to ensure that even when there is strong evidence of guilt, the defendant will be exonerated if there is a reasonable doubt in the judge’s mind. This is done by imposing a disproportionately high burden of persuasion on the government. The social conclusion that an individual’s liberty interest outweighs the state’s interest in securing a criminal conviction, or, as it is more commonly put, that it is much worse to convict an innocent man than to let a guilty man go free, is what

19 Authors study on the basis of news report of difffident dailies conducted from January, 2022 to August, 2023.
led to the deliberate imbalance in favour of the defendant. Thus, the constitutional meaning of the presumption of innocence is provided by the reasonable doubt test.

The presumption of innocence, which is a cornerstone of a fair and just legal system, is upheld by the theory of reasonable doubt. As the U.S. Supreme Court noted, "The principle that there is a presumption of innocence in favor of the accused is the undoubted law, axiomatic and elementary, and its enforcement lies at the foundation of the administration of our criminal law." The protection of reasonable doubt prevents the conviction of innocent people. This idea recognises that the criminal justice system is imperfect and that mistakes might happen during inquiries, witness interviews, and the presentation of the evidence. As Justice Jackson wrote in the case of In re Winship (1970), "Lives of persons are at stake and, if they are not to be held in detention or conviction except on the highest standards of proof, these standards must be insisted upon in prosecutions for all crimes." The existence of reasonable doubt serves as a check on state power by requiring a heavy standard of proof before the government may take away someone's freedom. In the words of Justice Harlan in the case of In re Winship (1970), "The reasonable-doubt standard plays a vital role in the American scheme of criminal procedure. It is a prime instrument for reducing the risk of convictions resting on factual error." Public confidence in the fairness and integrity of the criminal justice system is increased by the notion of reasonable doubt. People are more likely to trust the system when they think that criminals are not found guilty unless the evidence is solid and convincing. According to Justice Rehnquist, the requirement of a finding of guilt beyond a reasonable doubt was essential because it made the fact-finder realise how important it was to establish a near-certain subjective conviction of the accused's guilt. The theory of reasonable doubt encourages prosecutors to thoroughly investigate cases, present reliable evidence, and operate with integrity by imposing a high burden of proof on the prosecution. This aids the US courts in avoiding the use of flimsy or circumstantial evidence to resolve cases.

Proving guilty of an offence is comparatively not fully dependent on the physical or conventional evidence in the US. The digital evidence has a pivotal role in this regard. The use of online evidence in US courts has become increasingly prevalent and has seen several successes in recent years. Online evidence can include a wide range of digital information, such as emails, social media posts, text messages, and electronic documents. Social media platforms like Facebook, Twitter, and Instagram have provided valuable evidence in numerous cases. For instance, in the Drew case, the accused was convicted for her involvement in a

---

23 ibid.
25 In re Winship (n 21).
26 ibid.
cyberbullying case where evidence from *MySpace* was crucial. The court determined that Drew had harassed a teenage girl online under a fictitious persona, which led to the girl’s suicide. Drew’s online pursuits, including her chats and posts, were a major factor in her conviction. On top of that the E-mail correspondence has played a crucial role in various legal proceedings. In the case of *United States v. Enron Corp.*, emails were central to uncovering corporate fraud. These emails provided insights into the unethical practices at Enron, leading to convictions of several high-ranking executives. Digital evidence from computers and mobile devices has also been recovered and examined using digital forensics tools and procedures. In situations involving cybercrimes like hacking and identity theft, this evidence has proved crucial. The case of *United States v. Albert Gonzalez* is an example where digital evidence, including chat logs and data on hacked computers, played a crucial role in convicting Gonzalez for one of the largest data breaches in U.S. history. Additionally, surveillance cameras and online video platforms have provided critical evidence in criminal cases. For example, in the *Commonwealth v. Dookhan* case, surveillance footage was used to prove that a Massachusetts state chemist had tampered with evidence, leading to the wrongful convictions of numerous individuals. Online financial records and transaction data have been used to trace money laundering and financial fraud. In the *United States v. Ulbricht* case, evidence from *Bitcoin* transactions was pivotal in the conviction of Ross Ulbricht, the operator of the Silk Road, an online black market. Mobile device location data has been used to place suspects at specific locations during criminal activities. The U.S. Supreme Court ruled that the use of GPS tracking data in the investigation of a drug trafficking case amounted to a Fourth Amendment search, highlighting the significance of such digital evidence.

These examples demonstrate how online evidence has successfully been used in US courts to secure convictions, uncover fraud, and establish the facts of a case. However, it’s important to note that the admissibility of online evidence can sometimes be a subject of legal debate, and its use must adhere to established legal principles and procedures. Moreover, as technology continues to evolve, the role of online evidence in the legal system will likely continue to expand and evolve as well.


Obtaining online evidence from the United States under international law is a difficult process, and the ease of obtaining such evidence depends on several factors, including the specific legal framework, the nature of the evidence, and the

---

29 ibid.
31 ibid.
32 United States v. Albert Gonzalez [2010] Criminal No. 08-10223-PBS.
country making the request. The legal procedure by which the US government responds to foreign requests for digital information or evidence from US social media companies involves a complex interplay of domestic and international laws and treaties.

Many foreign requests for digital information or evidence from US social media companies are initiated through Mutual Legal Assistance Treaties (MLATs). MLATs are bilateral agreements that allow countries to request legal assistance from each other in criminal investigations and prosecutions. The U.S. has MLATs with numerous countries, and these treaties outline the process for making and responding to requests for evidence. US domestic law also plays a crucial role in responding to foreign requests. The Stored Communications Act (SCA), governs access to stored electronic communications and subscriber records by governmental entities, including foreign governments. To obtain data from US social media companies, foreign authorities may need to work within the framework of the SCA, which requires compliance with specific procedures and standards. Electronic Communications Privacy Act (ECPA) is also another relevant U.S. law that governs the interception and access to electronic communications and stored data. Requests for digital information from foreign states must comply with ECPA provisions, and the U.S. government’s response to such requests should adhere to ECPA requirements. In addition to MLATs, there are international agreements and conventions that may facilitate requests for digital evidence. For example, the Budapest Convention on Cybercrime is a multilateral treaty that addresses various aspects of cybercrime, including the preservation and sharing of electronic evidence across borders. While the U.S. is not a party to the Budapest Convention, it may still cooperate with parties to the convention on specific cases.

Procedure for request and reviewing them are always done on the basis of the US socio-legal values or US community standard not on the same of the country in need of the evidence. When a foreign government wishes to obtain digital information or evidence from US social media companies, it typically initiates the

---

38 Convention on Cybercrime [2001] (Budapest).
process by making a formal request through diplomatic channels or via an MLAT. The request should specify the information sought, the relevant legal basis, and details about the criminal investigation or prosecution in the requesting country. Upon receiving a foreign request, the U.S. government reviews it to ensure that it complies with US law and the relevant international agreements. The US Department of Justice and other agencies may be involved in this process. In some cases, a U.S. court may become involved if the request requires a court order for compliance. For example, if the request involves compelling a social media company to disclose certain information, a court order may be necessary under the SCA or ECPA. The court will evaluate the request based on US law and constitutional principles.

Once the request is approved and deemed lawful, US authorities will execute it, working in coordination with the relevant social media company to provide the requested digital information or evidence to the foreign government. It is important to note that the specific procedures and requirements can vary depending on the circumstances, the laws of the requesting country, and the details of the case. Additionally, considerations related to privacy, human rights, and the potential impact on freedom of expression may also factor into the decision-making process.

This process is no doubt a complexity of handling foreign requests for digital information and the need for a careful balance between international cooperation in criminal investigations and the protection of individual rights and privacy.

10. State Response on Digital Evidence: A Study on Facebook

Bangladesh is among the top three nations contributing active users growth for Facebook as of December 31, 2022, Meta said in a regulatory filing. The company has reported a 4% increase in worldwide daily active users (DAUs) to 2 billion on average during December 2022. The need for digital evidence from Facebook is accordingly increasing although there is no baseline research or statistical data in this regard. However, we can understand the issue with the previous two years request from Bangladesh to Meta for required information.

According to reports published by Facebook’s parent company Meta since January 2023, the number of requests from the Bangladesh government is gradually increasing. In 2022, the government of Bangladesh sought information about a maximum of 2,449 accounts or users. The news claimed that Meta provided 64.83% information. Bangladesh has sought more information from

---


42 ibid.
Facebook this year than before, according to the *Transparency Report*. From July through December of 2021, the government sent 525 requests. It was also claimed that Facebook responded by supplying 66.86% of the information. This calculation does not provide the actual percentage of supplied information. This is actually calculated in the number of users’ information not the amount of users’ data. It does not include deleted and altered data. Although it is claimed that *Meta* does not preserve any deleted *facebook* content more than 90 days, there is no guarantee or legal responsibility of permanently deleting users’ information. The US government may use all the evidence even it is deleted (after retrieving) if it is required in the US court. This position of *Facebook* brings a significant difference in the quality of justice in the US and in Bangladesh.

11. Procedural Challenges of Documentation of Online Evidence

Chain of custody and authentication are both in the centre of documentation of digital evidence. The procedure of authenticating evidence is used to confirm that it is what it claims to be. The person presenting the proof must prove that the object is authentic. Identifying the author of electronic records is frequently a crucial step in verifying digital evidence. For instance, the prosecution would have to provide evidence that the defendant actually wrote the email that was purportedly sent to the victim. The Federal Rules of Evidence (US), which many state courts have also adopted, permit authentication to be established through the testimony of an informed witness, such as a law enforcement officer who seized a computer or mobile device and can attest to where the files were taken from and matches of names in the files to other evidence gathered. Emails can be verified in a number of ways, such as proving they contain information the defendant would have known about or providing evidence that the defendant had main access to the equipment used to create the message. Radina Stoykova identifies three categories of unaddressed threats to fairness and the presumption of innocence during investigations namely, the inappropriate and inconsistent use of technology; old procedural guarantees, which are not adapted to contemporary digital evidence processes and services; and the lack of reliability testing in digital forensics practice.

---


44 ibid.


46 ibid.


48 ibid.

Inappropriate use of technology that has not been thoroughly tested affects the presumption of innocence at the beginning of an investigation and the right to a fair trial as outlined in the ECHR. The need for legal certainty in the judicial process and unfair treatment of suspects and defendants can result from an overreliance on and inappropriate use of technology combined with the precarious situation of suspects and defendants.\textsuperscript{49} The presumption of innocence in technology-assisted investigations is firstly challenged given the inappropriate and inconsistent use of technology. This creates issues, some of which are already examined in such as tunnel vision\textsuperscript{50} at an early stage of the investigation; lack of reliable and complete evidence; parallel construction of facts;\textsuperscript{51} lack of access to relevant evidence and forensic resources by the defence; unduly long retention of evidence and data on acquitted/suspected people for comparison. Here the debate is enriched with considerations on the need for transparency and accountability in digital investigations and applied reliability validation of the digital forensic techniques employed.

12. How ‘Reasonable Doubt’ Gets Unreasonably Affected in Digital Age

Access to online evidence held in foreign custody presents a significant challenge for law enforcement agencies and legal authorities worldwide due to jurisdictional complexities and privacy concerns. Online data is often stored on servers located in foreign countries. Determining which jurisdiction has the legal authority to access and obtain evidence stored on these servers can be a complex and contentious issue. This challenge is exemplified by the case, where Microsoft challenged a U.S. government warrant seeking access to email data stored on a server in Ireland.\textsuperscript{52} The case raised questions about the extraterritorial reach of US warrants and the sovereignty of foreign countries over data stored within their borders. Different countries have varying laws and regulations governing data privacy, data protection, and law enforcement access to online evidence. These conflicting legal frameworks can hinder the ability to obtain evidence. For instance, the European Union’s General Data Protection Regulation (GDPR)\textsuperscript{53} restricts the transfer of personal data outside of the EU, complicating cross-border data access. Accessing online evidence stored in foreign custody can raise privacy concerns, both for individuals and the companies that store user data. Cases like the one involving Facebook and Cambridge Analytica highlighted the importance of protecting user privacy and obtaining proper legal authorization to access personal data.

\textsuperscript{49} ibid.
\textsuperscript{52} Microsoft Corp. v. United States [2018] 138 S. Ct. 1186.
\textsuperscript{53} General Data Protection Regulation [2016] 679.
MLATs are agreements between countries that facilitate the exchange of evidence and cooperation in criminal investigations. While they are intended to streamline the process of accessing foreign-held evidence, MLATs is slow and bureaucratic. Delays in obtaining evidence through MLATs can impede ongoing investigations. Many online service providers use encryption to protect user data. This encryption can make it difficult or even impossible for authorities to access data, even with a valid legal request. High-profile cases, such as the Apple-FBI standoff over access to the iPhone of the San Bernardino shooter, illustrate the challenges posed by encryption in accessing evidence. There is a lack of standardized procedures and mechanisms for accessing online evidence in foreign custody. The absence of international norms or standards can lead to inconsistent and inefficient processes for obtaining evidence.

The arguments in this regard are not meant to refute the generalisation that convicting an innocent person unfairly causes more harm than clearing a guilty person of a charge. The conviction of the innocent is nearly always perceived as the larger injustice, regardless of whether the issue is one of morality, constitutionality, or public opinion. However, two issues are highly influential in digital evidence opportunity. First, accessing digital evidence in foreign jurisdiction not been practically recognized as rights even if no conflict of national interest is involved. Availability of digital evidence necessarily keeps a justice system ahead of those who do not have the same. Thus, quality of justice in non-privileged States does not become the identical to the privileged States.

13. Potentials of Localizing Overseas Digital Platforms and State Responsibilities

The localization of foreign digital platforms is a significant issue with far-reaching implications for ensuring justice in local courts. This phenomenon pertains to the adaptation of digital services provided by foreign tech companies to comply with the legal, cultural, and linguistic norms of the jurisdiction in which they operate. Localization enables individuals and entities within a jurisdiction to have better access to legal recourse in case of disputes involving foreign digital platforms. When these platforms are tailored to local standards and laws, it becomes easier for aggrieved parties to seek redress within their own legal system. This reduces barriers to justice and promotes fairness.

Digital platforms that are localized can better understand and respect the cultural nuances and linguistic diversity of the local population. This is crucial for ensuring that content moderation, user agreements, and dispute resolution mechanisms are culturally sensitive and do not inadvertently discriminate against

---

55 Apple–FBI Encryption Dispute Case [2015].
56 ibid.
certain groups or individuals based on language or cultural differences. Different jurisdictions have unique legal requirements, ranging from data protection and privacy regulations to hate speech and defamation laws. Localization ensures that foreign platforms adhere to these local legal frameworks, reducing the risk of legal conflicts and enabling a more harmonious coexistence between global tech companies and local legal systems.

Keeping digital evidence at a convenient location is crucial to ensure justice and is surely to have a significant impact on the evidentiary value of digital content in legal proceedings. Content that is translated and adapted to the local context is more likely to be considered relevant and admissible in local courts. This enhances the ability of the legal system to effectively adjudicate cases involving digital evidence. Localization can also improve users’ understanding of the terms and conditions, privacy policies, and dispute resolution processes of digital platforms. When users are better informed, they are more likely to engage with these platforms in a legally responsible manner and are better prepared to protect their rights in the event of disputes.

Localization reinforces the principle of jurisdictional sovereignty, whereby each country has the authority to regulate and adjudicate matters within its borders. This principle is essential for maintaining the rule of law and ensuring that local courts have the authority to address disputes involving foreign digital platforms operating within their jurisdiction. While localization is essential for respecting local laws and customs, it should also be done in a way that maintains a level of global consistency. Striking the right balance between localization and global standards is critical to ensuring that digital platforms can operate efficiently across multiple jurisdictions without compromising their commitment to justice and user rights. Therefore, the localization of foreign digital platforms is not only significant but also essential for ensuring justice in local courts. It helps bridge the gap between global tech companies and local legal systems, making it easier for individuals and entities to seek legal remedies, promoting cultural and legal sensitivity, and upholding the rule of law in an increasingly interconnected digital world.

14. Concluding Remarks

In wrapping up, the use of digital evidence in a foreign country and how it affects the level of justice in another country invite a complicated and developing landscape. For legal systems all around the world, the emergence of the digital age has brought both opportunities and challenges. Access to digital evidence across borders is critical for tackling cross-border crimes and ensuring justice in a connected society. However, a number of legal, technological, and political variables affect how simple it is to get such proof. Universal application of MLATs and other international agreements can make it easier for countries to work together to share digital evidence. However, inconsistencies in legislative
frameworks, worries about data privacy, and a range of technology capabilities may make it difficult to work together effectively.

The collection of digital evidence necessitates a cautious balancing act between the investigative needs of law enforcement and the rights of the individual, such as due process and privacy. Maintaining this equilibrium is essential for sustaining the rule of law and justice. The suitability of legal frameworks is constantly put to the test by the quick development of technology. In order to ensure that digital evidence is efficiently gathered, stored, and presented in a court of law, it is crucial to keep up with technological changes.

The handling of requests for digital evidence must be transparent, and impartiality must be promoted throughout the process. Mechanisms for accountability and supervision need to be in place to stop any abuses. A more equal and just legal environment can be achieved by promoting the creation of international standards and best practices for the management of digital evidence. Achieving these requirements requires international cooperation. Digital evidence and its use in other countries must be discussed with ethical considerations, such as preserving individual privacy and guarding against undue intrusion, at the forefront of the conversation.

Regardless of the digital nature of the evidence or its origin, the overarching goal must be to improve the quality of justice and respect the principles of fairness, due process, and individual rights. In a world where technology continues to redefine the borders of justice and jurisdiction, achieving this goal necessitates constant communication, collaboration, and adaptability. In the digital era, the quest for justice is a dynamic journey that calls for alertness, creativity, and a firm adherence to the values of justice and the rule of law discussions on the use of digital evidence in other countries are at the forefront.