Investigating the Legal Complexities of Cloud Forensic Investigations in Cross-Border Scenarios and Developing Strategies for International Cooperation

Francis Chidiebele Ekwempu

University of East London, London, UK

DOI: https://doi.org/10.51584/IJRIAS.2026.110100113

Received: 25 January 2026; Accepted: 30 January 2026; Published: 16 February 2026

ABSTRACT

Introduction: The rapid rise of cloud computing has reshaped data storage and crime, shifting investigations to digital forensics. Jurisdictional complexities, dispersed data, and lack of server access hinder cross-border cloud forensics, while no unified international legal framework allows cybercriminals to find safe havens and blocks admissible evidence preservation.

Objectives: This study aims to analyse the legal challenges hindering effective cross-border cloud forensic investigations and propose strategies for international cooperation. The key objectives of this study include identifying issues related to data sovereignty, jurisdiction, and evidence admissibility and establishing best practices to streamline multinational collaboration.

Methods: A case study analysis methodology was employed to examine complex legal phenomena in real-world contexts. A diverse dataset of high-profile cases, including United States v. Microsoft Corp., the Yahoo Data Breach, and Cambridge Analytica scandal This study also evaluates existing frameworks, such as the MLATs, the Budapest Convention on Cybercrime, and the CLOUD Act.

Results: The analysis reveals that existing legal mechanisms, such as MLATs, are often too slow for the digital age, sometimes taking months or years to complete. The findings underscore that legislative updates, such as the CLOUD Act, have begun to address access to extraterritorial data but often conflict with the GDPR. High-profile cases demonstrate that successful outcomes rely heavily on the cooperation of cloud service providers and the alignment of disparate domestic laws.

Conclusions: A standardised international legal framework is crucial for the future of cloud forensics. The research concludes that enhancing global cooperation requires a multi-faceted approach, including the automation of forensic tools, the establishment of 24/7 contact points between nations, and the harmonisation of national cybercrime and data protection laws to ensure both investigative efficiency and human rights protection.

Keywords: Cloud Forensics, Cross-Border Jurisdiction, Digital Evidence, International Cooperation, Data Privacy.

INTRODUCTION

Cross-border cloud forensic investigations are complicated because of jurisdictional difficulties, data ownership and custody, technical challenges, and differences in legal and procedural matters(Malik et al., 2024). Data can be held in many countries, each with its own legal system. This makes it hard to figure out who owns the data and to establish a clear chain of custody. Cloud settings are also dynamic, which makes it difficult to acquire and analyze data, and anti-forensic tactics may complicate investigations. Obtaining evidence might be delayed or made more difficult due to a variety of legal procedures and international cooperation systems(AllahRakha, 2024).

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

The Internet has significantly transformed cross-border crime investigations, from local to global issues. Prior to the internet, these investigations were primarily conducted through diplomatic channels, extradition treaties, and international cooperation agreements. An example of an extradition treaty is the Webster-Ashburton Treaty, which was signed between the United States and Great Britain (Dickson, 2024). However, the rise of the internet has necessitated a shift towards faster and more efficient investigative methods, underlining the pressing need to adapt to the digital age.

The key differences between cross-border criminal investigations in the pre- and post-Internet era are stark, particularly in jurisdictional boundaries, evidence, speed, and privacy issues. Investigations before the Internet were slow and laborious, relying on physical evidence and witness accounts. The advent of the Internet has necessitated a significant and urgent shift towards faster and more efficient investigative methods, underlining the pressing need to adapt to the digital age.

The limitations of traditional policing and law enforcement institutions like Interpol highlight the necessity of working together on a global scale (Lemieux, 2024). Variations in legal frameworks, cultural values, and levels of technical development caused significant disparities in how crimes were handled across borders. With the advent of the Internet, crime has transcended national borders, giving rise to cybercrime and digital fraud. The lack of robust international legal frameworks often exposes personal data across borders, leading to heightened privacy concerns. This underscores the crucial need for unified legal solutions on a global scale, such as Mutual legal assistance treaties (MLATs) which facilitates cooperation in criminal investigations and prosecutions, allowing for the exchange of evidence and witness testimony. The General Data Protection Regulation (GDPR) in the European Union (EU), also help to effectively combat the interconnectedness of modern crime and privacy violations (Ok et al., 2025).

The Internet's vast scale and rapid speed have given rise to new forms of crime such as hacking, phishing, and online fraud, affecting millions of individuals worldwide. The jurisdictional challenges it presents, coupled with the fact that offenders, victims, and servers are often located in different countries, further complicates the situation (Ashurov, 2024). The Internet's capability to collect, store, and transmit large volumes of personal data has also raised serious concerns about data protection and privacy.

Cloud forensics investigation is a complex task, fraught with difficulties due to the dispersed nature of data, the lack of physical access, evolving regulatory frameworks, and the necessity for international collaboration. The data, when distributed, is held in various jurisdictions, making it challenging to determine the location of evidence and the applicable laws. Investigators often lack direct access to cloud servers, necessitating reliance on the assistance of providers who are subject to different regulatory standards. The constantly changing laws and regulatins related to cloud computing and data privacy further complicate and obscure cross-border inquiries. Cross-border cloud forensic investigations encounter complicated legal issues, such as jurisdiction, sovereignty, and data privacy(Deandra & Sherly, 2025)**.** The United States v. Microsoft Corp. case is one of the most significant court cases. In this case, the United States wanted to access emails held on Microsoft's servers in Ireland. To do this, they invoked the Stored Communications Act (SCA). Microsoft argued that US warrants did not have the authority to be enforced outside the United States. In 2018, the legal landscape changed significantly with the passing of the Clarifying Lawful Overseas Use of Data (CLOUD) Act after the Second Circuit Court ruled in favor of Microsoft(Zuo, 2024). China has unique legal frameworks, such as Jian Li No.67, that regulate cross-border access to electronic data in criminal situations. These frameworks emphasize the importance of confirming the legitimacy and legality of electronic data that is obtained from foreign sources. As a result, the cases emphasize the significance of international collaboration and well-defined legal structures in successfully addressing these difficulties.

However, **t**he research topic explores the legal complexities of cloud forensic investigations in cross-border scenarios and developing international cooperation strategies. It delves into cybersecurity law, international law, cloud computing, and forensic science, focusing on digital evidence, surveillance, data privacy, and computer crimes(Ashurov, 2024). Cloud computing involves understanding cloud infrastructure and data storage challenges, while forensic science involves collecting, preserving, analyzing, and presenting digital evidence in legal proceedings. The research explores cross-border jurisdiction, data privacy laws, international cooperation, and technical challenges in cloud-based crimes. It aims to balance forensic investigations with

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

data privacy regulations, develop collaboration strategies, and address technical difficulties in cloud environments. It also aims to guide practitioners, policymakers, and cloud service users in navigating cloud-based investigations, establishing a comprehensive, legally admissible approach for conducting digital forensic examinations(Egho-Promise et al., 2024).

Research Problem:

The lack of a unified international legal framework for cloud forensic investigations in cross-border scenarios creates significant challenges in preserving digital evidence, ensuring jurisdictional clarity, and facilitating effective international cooperation. The lack of a unified international legal framework for cloud forensic investigations in cross-border scenarios is a significant issue due to the rapid growth and increasing reliance on cloud computing services(Alex & Kishore, 2017). The lack of an identical international legal framework might impair investigations, law enforcement cooperation, and cloud service confidence. Ambiguity can make cybercrime investigations harder, cloud service confidence lower, and international cooperation lower. A unified legal framework is urgently needed to explain jurisdiction, enable cooperation, and preserve digital evidence.

Due to the cross-border nature of cloud services, there is no standardized international legal framework for cloud forensic investigations in cross-border contexts, which makes digital evidence preservation difficult, creates jurisdictional ambiguity, and hinders international cooperation. The lack of a unified legal framework can hinder effective collaboration between law enforcement agencies, thereby limiting the investigation and prosecution of cybercrimes(Alex & Kishore, 2017). Therefore, a standardized international legal framework is crucial for effective cloud forensic investigations.

The project seeks to comprehend cross-border cloud forensic investigations' legal challenges and establish international cooperation techniques. International treaties, domestic laws, and data protection requirements will be examined(Casino et al., 2022). The research will identify data sovereignty, jurisdiction, admissibility, and international collaboration issues in cross-border cloud forensic investigations. Following the analysis, the research will propose standards, procedures, or best practices for multinational cloud forensic investigations to ease cross-border collaboration and ensure legality and efficiency(Olber, 2021). This legal overview will help law enforcement, legal experts, and policymakers investigate international digital crimes.

Theoretical framework

The move to cloud computing has complicated legal, regulatory, and technical issues, especially in forensic investigations of cloud data across jurisdictions(Malik et al., 2024). The theoretical framework for cloud computing focuses on three core areas: cloud computing architecture and data governance, digital forensics and cross-border data investigations, and international law and sovereignty in cybercrime. Cloud computing operates on a distributed model, presenting unique challenges in determining the jurisdiction of stored data. Data governance, such as ownership, access control, and regulatory compliance, are crucial in cross-border scenarios (Malik et al., 2024). Digital forensics differ from traditional forensics in terms of evidence preservation and cloud readiness. The Digital Forensic Process Model and Cybercrime Investigative Theory outline the stages of digital investigations(Sibe & Kaunert, 2024). International law and sovereignty are crucial in cloud environments, as data moves across borders. Strategies for international cooperation include multi-stakeholder governance models, rapid response mechanisms, International Regulatory Cooperation, and Network Theory in International Relation(Michels et al., 2023).

Aims

Research aims to understand legal complexities, jurisdictional issues, data privacy laws, international cooperation, evolving threats, and best practices for conducting investigations. To analyze the legal challenges hindering effective cross-border cloud forensic investigations and to propose strategies for enhancing international cooperation to overcome these obstacles.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

The gap between technological advancements and forensic techniques is widening, causing cybercrimes, public trust erosion, and data exploitation. To address this, a future-oriented approach involving automation, AI, ML, cloud-based forensics, and continuous adaptation is needed. Automated tools automate evidence collection, analysis, and reporting, while AI-powered analysis identifies suspicious patterns and uncovers hidden digital evidence. Cloud-based forensics use multiple platforms for efficient investigations, resulting in faster, more accurate investigations, enhanced collaboration, and reduced costs(Nelufule et al., 2024).

Cloud computing is increasingly important for data storage and processing, but it also poses challenges such as cybercrime targets, jurisdictional issues, and conflicting legal frameworks. Effective international cooperation is crucial for sharing evidence and fostering trust in cloud services. Research on legal complexities and international cooperation can help navigate these challenges and promote a secure digital world.

LITERATURE REVIEW

Cloud computing has revolutionized data storage and processing. However, it presents significant challenges for forensic investigations, particularly when data crosses multiple jurisdictions. This literature review delves into the legal complexities of cross-border cloud forensic investigations and explores solutions for international collaboration. It identifies gaps in current frameworks, proposes potential remedies, and discusses strategies to enhance international collaboration in addressing these challenges. It underscores the urgent need for ongoing research and brings hope and optimism about the potential remedies to the identified gaps.

Some of the recent research in cloud forensic investigation in cross-border scenario include Legal challenges in digital forensics for financial crime investigations**;** Demystifying the Network and Cloud Forensics' Legal, Ethical, and Practical Considerations; Cloud digital forensics: Beyond tools, techniques, and challenges; Digital forensic investigation in cybercrime cases: case studies and recommendations; Advancing digital forensic investigations: addressing challenges and enhancing cybercrime solutions; The Impact of Cybersecurity Laws on Legal Procedures and Case Law; and The need for cybercrime regulation on a global scale by the international law and cyber convention.

Legal challenges in digital forensics for financial crime investigations; the research employed a mixed-methods approach to analyze the legal intricacies of digital forensics in financial crime investigations. It elucidates substantial obstacles and methodologies for enhancing efficacy. The results underscore the necessity for standardization, global collaboration, and continuous training to improve digital forensics' legal and operational effectiveness in financial crime investigations(Ozioko, 2024).

Demystifying the Network and Cloud Forensics' Legal, Ethical, and Practical Considerations; the study investigates network and cloud forensics through qualitative methods and grounded theory, highlighting deficiencies in liability constraints, ethical data acquisition, and anti-forensic concealment strategies. The proposed solutions underscore the crucial role of the audience in advancing cybersecurity, encompassing transparency in technological design, the simplification of cross-border legal aid protocols, the development of lightweight encryption techniques, and the enhancement of collaboration between businesses and academics(AllahRakha, 2024).

Cloud digital forensics: Beyond tools, techniques, and challenges; this study delves into the challenges of protecting and enhancing data within the cloud environment, evaluating data breaches and their economic implications. It also compares traditional digital forensics with cloud computing-specific forensic methodologies. The study's findings not only point towards promising research directions but also have practical implications, deepening our understanding of cloud data protection and security. The compound annual growth rate (CAGR) of cloud digital forensics is projected to be 16.53% from 2023 to 2031, with the market expected to reach approximately USD 36.9 billion by 2031. The paper explores emerging issues in cloud digital forensics, offering a comprehensive roadmap for navigating and overcoming the complexities of the evolving cloud computing landscape(Annas et al., 2024).

Digital forensic investigation in cybercrime cases: case studies and recommendations; this study examines the application of digital forensic techniques in addressing cybercrime occurrences, utilizing case examples to

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

underscore its advantages and drawbacks. It offers a comprehensive understanding of the interdisciplinary nature of digital forensics, incorporating computing, legal frameworks, and investigative methodologies(Syaakirah et al., 2025).

Advancing digital forensic investigations: addressing challenges and enhancing cybercrime solutions; the research underscores the significance of systematic forensic methodology, informed by international standards such as ISO 27037:2012, in refining forensic procedures and advancing cybercrime investigations. It particularly emphasizes the role of digital forensics in enhancing cybersecurity, thereby providing a sense of security and protection. Digital forensics also plays a key role in reconstructing criminal incidents and facilitating legal processes through credible evidence, especially with encrypted communications, cloud infrastructures, and decentralized data storage(Deandra & Sherly, 2025).

The Impact of Cybersecurity Laws on Legal Procedures and Case Law; this study critically examines the influence of cybersecurity legislation on legal structures, judicial processes, and case law, a topic of utmost relevance to legal professionals, cybersecurity experts, and academics. It analyzes significant regulations such as GDPR and the Cybersecurity Act and their implications for evidence management, litigation tactics, and liability. The article explores innovative legal theories, the complexities of interpreting cybersecurity legislation, jurisdictional challenges in transnational cases, the pivotal role of digital forensics, the application of expert testimony in cyber-related trials, and the ever-evolving nature of cybersecurity threats, fostering a sense of connection and involvement in the reader(Ok et al., 2025).

The need for cybercrime regulation on a global scale by the international law and cyber convention; this study emphasizes the importance of controlling cybercrime using International Law Principles and treaties as the legal foundation for international cybercrime legislation. The implications of cybercrime in cyberattack events are based on known cyberattack behaviors and literature, highlighting the imminent nature of these threats. The Convention on Cybercrime, established in Budapest in 2001, is a pivotal international agreement addressing cybercrime and electronic evidence. Countries across Africa, the Americas, and the Asia/Pacific are harnessing this agreement to implement robust strategies against cybercrime. Cybercrime is a new area of international law, namely International Criminal Law, and it is urgent to govern it globally. The study employs a comprehensive approach, merging normative legal research with comparative legal analysis both within the European Union and globally, instilling confidence in the research methodology. Policy analysis is conducted to assess existing strategies and critically propose innovative solutions. At the same time, technological insights are integrated to ensure legal frameworks are attuned to the rapidly evolving landscape of cyber threats(Buçaj & Idrizaj, 2025).

Research justification in context of existing knowledge

Investigating the legal complexities of cloud forensic investigations in cross-border scenarios is crucial due to the confluence of several critical factors. The lack of international cloud forensics standards causes legal and practical issues in evidence admissibility, investigative techniques, and legal interpretations across jurisdictions. Cloud computing and rapid technical breakthroughs require continual legal framework revisions, generating ambiguity and complexity for international investigators. Cybercrime, including ransomware attacks, data breaches, and IP theft, is increasingly multijurisdictional and uses cloud services. Because cybercrime is global, forensic investigations must be coordinated across borders. Cloud forensics investigations are complicated by AI, blockchain, and IoT, but they may also improve capabilities. Addressing cross-border cloud forensics legal issues improves cyberspace security and best practices. Legal clarity and international cooperation streamline cross-border forensic investigations, reducing delays. As Böhm (2021) highlights, recent cyberattacks have underscored the urgent need for robust cross-border cooperation in forensic investigations. Effective cooperation requires clear legal frameworks, standardized procedures, and efficient mechanisms for mutual legal assistance.

As Ozioko (2024) emphasizes, standardization, global collaboration, and continuous training are crucial for improving the legal and operational effectiveness of digital forensics in financial crime investigations, particularly in the cloud environment. The call for improved accountability in technology design (AllahRakha, 2024) recognizes the need to develop technologies with forensic considerations in mind. Simplifying cross-

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

border legal assistance requests is essential for facilitating timely and effective cooperation between jurisdictions. The research by Annas et al. (2024) highlights the need for a comprehensive strategy to address the intricacies of the evolving cloud computing environment, emphasizing the importance of understanding the foundational concepts and techniques of digital forensics (Syaakirah et al., 2025). The challenges in interpreting cybersecurity laws, particularly concerning jurisdictional issues in cross-border disputes (Ok et al., 2025), further justify the need for clear legal frameworks and international agreements. Establishing international cybercrime laws based on principles and treaties of international law (Buçaj & Idrizaj, 2025) underscores the need for a global approach to combating cybercrime in the cloud.

Legal frameworks

Due to regulatory frameworks, stakeholders cannot easily share digital evidence in criminal investigations. Time restrictions complicate cross-border investigations. This article examines cross-border investigations' collaboration protocols and obstacles. It addresses these difficulties from a practical, global viewpoint, allowing practitioners and stakeholders to use horizontal solutions to quickly and precisely fill gaps (Casino et al., 2022).

The International Association of Computer Investigative Specialists (IACIS) Framework is a versatile collection of recommendations and best practices for conducting cloud forensic investigations across international borders(Safie & Bin Md Bashah, 2024). Its adaptability allows it to be tailored to the specific challenges of cross-border cloud forensics, considering factors such as data sovereignty, jurisdictional complexities, and international cooperation. The NIST Cybersecurity Framework, on the other hand, is a set of voluntary cybersecurity standards and best practices that can be used to assess the cybersecurity posture of cloud service providers and identify potential vulnerabilities that could impact cross-border investigations(Toussaint et al., 2024).

The DAMA-DMBOK (Data Management Body of Knowledge) framework provides principles and best practices for managing data throughout its lifecycle(Sargiotis, 2024). It analyzes how data is acquired, stored, and processed on the cloud and how these procedures can affect investigations that traverse international borders. A custom framework may be established depending on the exact goals and extent of the investigation.

When conducting a comprehensive analysis of high-profile cases involving cross-border cloud forensics, several factors must be considered. These include the legal and regulatory frameworks in the countries involved, the technical difficulties that arise when collecting and analyzing data from cloud environments, the role that cloud service providers play in either facilitating or obstructing investigations, and the effects of international cooperation and data-sharing agreements(Alshabibi et al., 2024). However, it's equally important to consider the ethical implications of cross-border data access and surveillance, as these can significantly impact the outcome of an investigation.

Several frameworks and models are frequently used when exploring the legal complexity of cloud forensic investigations, especially those that involve cross-border issues. Some examples are the NIST Cloud Computing Forensic Science Challenges Framework, the Council of Europe's Budapest Convention on Cybercrime, ISO/IEC 27037: Guidelines for Evidence Handling, INTERPOL Global Guidelines for Digital Forensics, Cross-Border Data Request Frameworks (such as the CLOUD Act and MLATs), and the SWGDE Framework. In high-profile instances, these frameworks are frequently used together, which assists investigators in dealing with problems such as data ownership, chain of custody, privacy laws (for example, GDPR), and CSP compliance standards.

Legal complexity, lack of standardization, rapid technological improvements, jurisdictional uncertainty, limited empirical evidence, data localization rules, contradictory regulations, technical complexity, and privacy issues complicate cross-border cloud forensic investigations. The report underlines the necessity of cloud service provider-based solutions for cloud forensics investigators, but also the potential impact of a new forensic evidence collection strategy outside the cloud. This strategy could significantly reduce the reliance on cloud-based solutions and the potential for data alteration, making its adoption urgent (Alex & Kishore, 2017).

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

Gap Filled

The research explores the legal complexities of cross-border cloud forensic investigations, addressing factors like data localization, cybercrime, jurisdiction, legal frameworks and digital evidence. It aims to analyze these complexities, develop strategies for international cooperation, and provide policy recommendations for governments and organizations. The goal is to improve efficiency in cross-border cloud forensic investigations and protect digital evidence.

METHODOLOGY

Experimental design:

Case Study Analysis: A case study analysis is necessary for cross-border cloud forensic investigations. This case-by-case approach permits multi-faceted investigations of complicated issues in their actual contexts. Many in the fields of business, law, and policy have come to appreciate the value of case studies as a means to better understand complex issues, events, and phenomena by observing them in their native, real-world settings(Crowe et al., 2011).

Case study analysis is a valuable research design for understanding complex phenomena within their real-world context. It involves an in-depth investigation of a specific case or a small number of cases to provide detailed insights. In cross-border cloud forensics, case study analysis can be particularly useful for examining specific incidents of cybercrime involving cloud services, understanding legal and procedural frameworks, and evaluating forensic tools and techniques. Advantages of case study analysis include in-depth understanding, contextual analysis, and identification of best practices. However, it's crucial to maintain scientific integrity and a rigorous, objective approach, as the potential for bias can influence data selection and interpretation. Other limitations include limited generalizability and the resource-intensive nature of the process. Findings from a specific case may not be generalizable to all cross-border cloud forensic investigations. In conclusion, case study analysis is a relevant and valuable research design for exploring the complex nature of cross-border cloud forensic investigations, contributing to the development of effective strategies, best practices, and legal frameworks for addressing challenges in this field.

Case Study Selection:

A range of high-profile cases involving cross-border cloud forensic investigations were carefully selected to ensure a diverse and comprehensive dataset. This diversity instills confidence in the reader about the breadth of the research. To achieve this, a structured framework is provided around key dimensions that represent the core legal complexities, underscoring the process's reliability and importance. It includes a case name, the nature of the crime, the data's location, the service provider's jurisdiction, the requester's jurisdiction, the key legal challenges, the key issues, the specific legal framework involved, the impact on the Investigation, and the outcome of the resolution.

Backgrounds of some high-profile cases

The Microsoft Ireland case (2013-2018)

A US appeals court case, United States v Microsoft, has rekindled a controversial international law question: can a state force a person on its territory to obtain and produce material owned or controlled by the person on its territory, stored on the territory of a foreign state? The case involved electronic data stored offshore for criminal prosecution. State practice reveals that unsanctioned cross-border evidence gathering is seen as an intrusion on territorial sovereignty, extending to the Microsoft Ireland case(Currie, 2017)**.** The Microsoft Ireland case (2013-2018) was a landmark legal dispute that significantly impacted the global legal landscape. It involved a compelling conflict between the United States law enforcement and Microsoft, a multinational technology firm based in the United States. The Department of Justice (DOJ) issued a warrant under the Stored Communications Act (SCA) to compel Microsoft to reveal emails relevant to an investigation into drug trafficking. However, Microsoft argued that US warrants should not have extraterritorial reach, and that

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

seizing data housed in another country would violate international law and the sovereignty of Ireland. They insisted that the Department of Justice should use a Mutual Legal Assistance Treaty (MLAT) with Ireland to obtain the data, sparking a legal battle of significant importance(Zuo, 2024).

The case directly challenged the United States domestic legislation (SCA) and the international legal principles that govern jurisdiction and data protection. The most important legal issues included extraterritoriality, data sovereignty, mutual legal assistance, and privacy rights. The matter went through multiple courts before it was finally brought to the United States Supreme Court. However, before the Supreme Court could decide, the United States Congress approved the CLOUD Act in 2018. This Act, a pivotal moment in the legal history of data access, changed the SCA to give US law enforcement the authority to seek data from US-based companies, no matter where the data is stored. The CLOUD Act has significantly altered the legal environment for accessing data across borders, underscoring the need for international collaboration and transparent legal frameworks in a globalized world(Christakis, 2017). In the context of law enforcement's access to digital data kept in other countries, the key concerns of data sovereignty, jurisdiction, and international legal frameworks were implicated. The issue revolved around the email data of a Microsoft customer that was kept in a data center in Dublin, Ireland. Even though the material was housed outside the United States, the US authorities attempted to obtain access to it as part of a criminal investigation. The Department of Justice (DOJ) contended that Microsoft was required to comply with the demand because it had authority over the data from the United States, regardless of where it was stored.

The CLOUD Act, a significant piece of legislation, clarified US law, allowing the Department of Justice to access data kept abroad by US corporations while also fostering international cooperation(Tréguer, 2018). The Act created reciprocal arrangements allowing countries to access each other's data legally, emphasizing the importance of international collaboration in the digital age. This included a later deal between the United States and the United Kingdom. Once the CLOUD Act was passed, the Department of Justice (DOJ) revoked its previous warrant and made a fresh request within the changed legal framework, which resolved the disagreement, highlighting the power of global legal cooperation.

Yahoo Data Breach (2013-2014)

Between 2013 and 2014, Yahoo experienced a significant cyberattack known as the Yahoo Data Breach. This incident exposed personal information, including names, email addresses, phone numbers, birth dates, encrypted passwords, and answers to security questions(Trautman & Ormerod, 2016). The breach was linked to Russian intelligence services, indicating that it was a cyber-espionage operation sponsored by the state to acquire intelligence and maybe for political objectives. Some of the stolen data was sold on the dark web, which puts users at risk of identity theft, phishing attempts, and fraud. With 3 billion accounts compromised, this is one of the worst data breaches in history(Tripathi & Mukhopadhyay, 2022). The Computer Fraud and Abuse Act (CFAA), the Stored Communications Act (SCA), the Federal Trade Commission (FTC) Enforcement, Mutual Legal Assistance Treaties (MLATs), and data protection regulations were all part of the legal framework for Yahoo Data Breach(Vogt, 2017). Civil settlements made under U.S. consumer protection statutes claimed that Yahoo was negligent in safeguarding user data.

Yahoo's late revelation of the breach made it challenging to access information, and connecting the attack to state-sponsored actors required advanced forensics and international cooperation. Yahoo became more exposed due to geopolitical issues, political tensions between the United States and Russia, and technological challenges. The breach had legal implications, including charges against four people, two of whom were Russian intelligence officials, and a settlement of $117.5 million in 2019 (Patterson, 2020). The leak also significantly impacted Yahoo's reputation and value around the time Verizon was acquiring the company. Cybersecurity awareness was raised, and the case highlighted the significance of suitable encryption methods, timely breach disclosure, and regular security audits for businesses.

Uber Hack (2016)

The Uber hack of 2016 was a significant cybersecurity incident that included unauthorized access, data location, and several jurisdictions. The attackers took advantage of a weakness when Uber developers

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

accidentally posted code containing credentials on GitHub. This is illegal under laws such as the Computer Fraud and Abuse Act (CFAA) in the United States and similar regulations in other countries. The stolen data was stored on Uber's servers, mainly in the United States. However, the data was likely stored in other countries' data centers. This incident underscores the critical importance of robust data security measures and the potential risks of unauthorized access and data breaches, even in well-established companies like Uber. The breach of 2016 had a profound impact on almost 57 million riders and drivers, whose personal information, including names, email addresses, phone numbers, and license numbers for some drivers, was compromised. The data was stored on Amazon Web Services (AWS), Uber's main cloud service provider. The incident revealed the challenges of exploiting poor access controls and exposing sensitive information stored in the cloud. The widespread nature of cloud storage made it difficult to identify all the affected systems and data, underscoring the human cost of cybersecurity incidents(McGovern, 2024).

The Federal Trade Commission (FTC) investigated Uber's data security standards and how the firm responded to the breach. The FTC's investigation was part of its broader efforts to enforce data security and consumer privacy laws(Robbins & Sechooler, 2018). Meanwhile, the United States Department of Justice (DOJ) attempted to seek criminal charges against the hackers. The DOJ's involvement highlights the serious legal consequences that can result from cybercrimes. Other countries, such as those in Europe covered by the General Data Protection Regulation (GDPR) or its predecessor, may have conducted their investigations or collaborated with authorities in the United States. Uber's inadequate data security and misleading claims about data protection were addressed through the employment of US rules, notably the FTC Act, state data breach reporting statutes, and the Computer Fraud and Abuse Act (CFAA).

In 2018, Uber negotiated a settlement of $148 million with all 50 states in the United States and the District of Columbia for not revealing the breach(Brown & Peterson, 2022). Uber was also fined £385,000 by the UK's Information Commissioner's Office and €600,000 by the Dutch Data Protection Authority(Islam & Karim, 2022). In response to the incident, Uber implemented significant changes to its data security measures. These included tighter data security safeguards, improved encryption, better access limits, and a more transparent security program. These changes demonstrate Uber's commitment to improving its data security and may serve as a model for other companies facing similar challenges.

Facebook-Cambridge Analytica case (2018)

The Facebook-Cambridge Analytica case involved a complex set of actions that raised serious ethical and legal concerns regarding data privacy, consent, and using personal information for political purposes. The issues involved improper data acquisition, misuse of data for political targeting, and lack of transparency and control over user data(Machova, 2021). The main service provider was Facebook, Inc. (now Meta), headquartered in the United States. Cambridge Analytica was a UK-based company with ties to the US (having a US subsidiary). This added another layer of jurisdictional complexity. The primary focus of investigations and legal actions was on the data held by Facebook in the US.

The service provider jurisdiction was Facebook, Inc. (now Meta), headquartered in the United States. Cambridge Analytica was a UK-based company with ties to the US (having a US subsidiary). Aleksandr Kogan's company, Global Science Research (GSR), which developed the 'This Is Your Digital Life' app, was also relevant. GSR was the entity that collected and shared the data with Cambridge Analytica. Kogan, a researcher at the University of Cambridge in the UK, was the key figure in this data collection process. The primary focus of investigations and legal actions was on Facebook's data held in the US. The main service provider Jurisdiction was Facebook, Inc. (now Meta), headquartered in the United States. Cambridge Analytica was a UK-based company with ties to the US (having a US subsidiary). The case's global impact, involving millions of users worldwide, made it challenging to establish jurisdiction. Key investigating bodies included the UK Information Commissioner's Office (ICO), the US Federal Trade Commission (FTC), and various EU data protection authorities, underscoring the widespread implications of the issue and the need for a global response(Verma et al., 2021).

The case outcome was a record $5 billion settlement with the FTC for its privacy violations, marking one of the largest penalties ever imposed by the FTC(Hazlett, 2023). The ICO fined Facebook £500,000 for breaches

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

of UK data protection law(Jougleux, 2022). Facebook and Cambridge Analytica suffered significant reputational damage, with Facebook's CEO, Mark Zuckerberg, being summoned to testify before the US Congress and Cambridge Analytica shutting down its operations.

Legal Frameworks

The relevant aspects of the body of laws which governs the relationships between states and includes treaties, conventions, and customary law as related to the chosen high-profile cases.

International and Domestic laws:

The legal frameworks considered under international laws in this study are Mutual Legal Assistance Treaties (MLATs), Data Protection & Privacy Laws, and Cybercrime Conventions. MLATs, crucial agreements between countries, play a pivotal role in facilitating cross-border criminal investigations. However, domestic laws related to evidence admissibility, search and seizure, and data privacy play a crucial role in cross-border investigations. Conflicts between domestic laws can create significant hurdles for investigators(Ashurov, 2024).

MLATs enable nations to assist each other in accessing digital evidence stored in other countries, a key aspect of modern law enforcement. Data privacy laws such as the GDPR serve as robust legal frameworks, providing a shield to protect people's personal information (data) from misuse, unauthorized access, or breach. These laws also empower individuals, ensuring they have control over how their data is collected, processed, stored, and shared, instilling a sense of security and reassurance. The Budapest Convention on Cybercrime (2001) holds the distinction of being the first international pact to address cybercrime and the cross-border access to data. Its establishment marks a significant milestone in the global fight against cybercrime, enlightening us about its historical significance(Gruber & Robin Pierce, 2019).

Processes required for obtaining MLATs and Cybercrime Conventions:

However, several important processes are involved in acquiring evidence through Mutual Legal Assistance Treaties (MLATs) and Cybercrime Conventions. Firstly, law enforcement authorities must establish if an MLAT is warranted, which often involves determining whether the evidence sought is in a foreign jurisdiction and whether domestic legal avenues are insufficient. The process will be governed by the specific MLAT between the requesting and requested countries. This will outline the sorts of help available, the procedures for making requests, and the constraints on aid. The request must include the following information: the identification of the authority making the request, the subject matter and type of the investigation, a summary of the relevant facts, and a description of the assistance being sought. Usually, the request is sent through diplomatic channels, which are commonly the Ministries of Justice or Foreign Affairs of the countries involved. The authorities of the country that was requested will examine the request and decide whether or not to carry it out. This may require judicial processes in the requested country to gather the proof. After the evidence is collected, it is sent back to the country that requested it through diplomatic means(Sharma, 2020).

Cybercrime conventions, like the Budapest Convention on Cybercrime, offer a structure for countries to work together in investigating and prosecuting cybercrime. These accords frequently contain clauses that address cross-border computer evidence, data retention, and international collaboration methods. On the other hand, the MLAT process can take a longer time, sometimes requiring months or even years to finish. MLATs are built on the principle of reciprocity, which means that governments are required to provide aid to each other in a reciprocal manner(Sharma, 2020).

In order to obtain MLATs and join cybercrime conventions, it is important to note the following steps as outlined below:

i. **Negotiation Phase:** Identifying the necessity for collaboration in legal matters, notably for handling transnational crimes.

ii. **Diplomatic Engagement:** Negotiations are started between two countries or among multiple countries, and legal representatives from the countries concerned negotiate the extent of the treaty.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

iii. **Drafting and Agreement:** Legal and policy experts from each country work together to develop the treaty's text. This text includes the scope of mutual aid, limitations, methods for submitting and processing requests, and data privacy and sovereignty safeguards.

iv. **Ratification:** The process of governments approving the agreement, exchanging ratification documents, and putting it into effect.

FINDINGS

A dataset was created to reflect the legal complexities of cross-border cloud forensic investigations, emphasizing the diverse factors that influence such cases as shown in **Table 1**. The examination of specific case studies provides valuable insights into the origins and emergence of these legal complexities, underscoring the indispensable role of international cooperation in such investigations. The background of the high-profile cases, the case name, the nature of the crime, the data's location, the service provider's jurisdiction, the requester's jurisdiction, the key legal challenges, the key issues, the specific legal framework involved, the impact on the Investigation, and the outcome of the resolution all point to the necessity of global collaboration.

Table 1. Dataset reflecting the Legal complexities from the selected high-profile cases

Case Name	**Nature of Crime**	**Data Location**	**Service Provider Jurisdiction**	**Requesting Jurisdiction**	**Key Legal Challenges**	**Key Issues**	**Specific Legal Framework Involved**	**Impact on Investigation**	**Resolution /Outcome**
The Microsoft Ireland Case (2013-2018)	Drug trafficking investigation	Ireland	United States	United States	Jurisdictional conflict; Extraterritorial application of UK law; Conflict with EU data protection (GDPR)	Jurisdiction, Sovereignty, Data Privacy	United States: Stored Communications Act **(SCA)**, *Clarifying Lawful Overseas Use of Data* **(CLOUD) Act**; Irish and EU Data Protection Laws: General Data Protection Regulation **(GDPR)**	Microsoft's warrant defiance delayed evidence availability, *highlighting the insufficiency of existing legal frameworks*, as the CLOUD Act authorized U.S. warrants for overseas data.	The US Supreme Court dismissed a case concerning Microsoft, which was initially accepted but terminated in 2018 owing to the CLOUD Act. In accordance with the new legislation, Microsoft adhered to the warrant, allowing law enforcement to acquire the data.
Yahoo Data Breach (2013-2014)	Cybercrime (unauthorized access to computer systems and theft of data)	USA & Others	USA	U.S. (FBI)	Russia did not extradite the FSB personnel, showing international law enforcement cooperation limitations.	Evidence Sharing, Extradition, Cybercrime	The Computer Fraud and Abuse Act (CFAA), the Stored Communications Act (SCA), the Federal Trade Commission (FTC) Enforcement, Mutual Legal Assistance Treaties (MLATs),	Complex attribution, huge breaches, and international collaboration between US and foreign law enforcement agencies to trace attackers and determine the breach's scope are investigation obstacles.	Hacker prosecution results in fines, settlements, regulatory changes, and unsolved Russian extradition concerns.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

Uber Hack (2016)	Cybercrime (Unauthorized access to cloud systems, data theft, and extortion)	USA	USA	UK, US	Uber's delayed notification of compromised credentials complicated investigations and penalties in many jurisdictions, underscoring breach disclosure law variations	Data Breach Reporting, Jurisdictional Compliance	U.S. Federal Trade Commission Act; Computer Fraud and Abuse Act (CFAA) EU General Data Protection Regulation **(GDPR)**	Uber's global breach required collaboration across regions with different notification rules and delayed notice, hindering legal measures.	Uber paid $148 million in settlements to US states and £385,000 to UK ICO for data breach notification violations, raising global awareness of breach notification requirements.
Facebook-Cambridge Analytica (2018)	Data privacy violation and unauthorized data use for political manipulation.	USA	USA	UK, USA, EU	Multiple jurisdictions conducting parallel investigations create coordination and data traceability concerns, requiring forensic investigators to assess data sharing, storage, and political profiling.	Consent, Privacy, International Regulations	EU General Data Protection Regulation **(GDPR)**; U.S. Federal Trade Commission Act (FTC Act); UK Data Protection Act **(DPA)** 1998/2018	The usage of Facebook's APIs to harvest user data from several countries caused jurisdictional and coordination concerns and complicated cloud forensics under opaque agreements.	Facebook's $5 billion FTC settlement and £500,000 ICO penalties for failing to protect user data sparked tougher API regulations and global data privacy discussions.

The dataset identifies the most important legal difficulties that arise while dealing with data. These are complex issues that require the expertise and involvement of legal professionals, data protection officers, and compliance teams. They include data privacy and protection concerns, jurisdictional conflicts, and challenges with mutual legal assistance (MLA). Another issue is the rights of data subjects, which include the right to access, the right to rectification, and the right to removal. Another issue is the constraints on data transfer across borders, which include regulations that require data to be stored in the country where it is collected and the Schrems II verdict. The e-Evidence Regulation (EU) and its methods provide safeguards for fundamental rights in direct access procedures but contradict national procedural regulations. The chain of custody and admissibility of evidence are also important challenges. This includes establishing a safe and reliable chain of custody in cloud environments, authenticating digital evidence across borders, and assuring admissibility in diverse legal systems.

However, a framework based on international and comparative law was considered since it concentrated on jurisdictional conflicts, data privacy and protection legislation, international legal instruments, legal assistance and mutual legal assistance treaties (MLATs), and changing legal frameworks. The impact of jurisdictional conflicts on cross-border investigations is significant, and it is crucial to address these conflicts to ensure smooth and effective investigations. Using a comparative law approach, a systematic comparison of legal frameworks across different jurisdictions was observed, highlighting similarities, variations, and potential conflicts. An international law framework, which applies international treaties, conventions, and customary international law to cross-border cloud forensics, played a crucial role in this context.

Analysis on key international laws for the cloud forensic investigations on the selected high-profile cases

The Microsoft Ireland case (2013-2018)

a) **Mutual Legal Assistance Treaties**: Mutual Legal Assistance Treaties: The US government's MLAT questioning in the Microsoft-Ireland case underscored the need for strong MLATs. The US tried to

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

impose a domestic warrant on Irish data without an MLAT, but the case showed the need of these agreements for cross-border data requests that respect local laws and sovereignty. Microsoft's support for MLATs as the legal basis for accessing foreign data strengthened this(Zuo, 2024). The case also highlighted MLATs' lengthy process and jurisdictional disputes, which complicate cross-border data access.

b) **Data Protection & Privacy Laws:** The case exhibits a clash between US law enforcement and European data protection laws, particularly the GDPR, which has significantly influenced cross-border data access laws. These laws now strive to strike a balance between law enforcement needs and privacy rights. Microsoft's refusal to comply with the warrant, citing the EU's strong emphasis on privacy and data sovereignty, which clashed with US regulations like the SCA, is a clear demonstration of the lack of harmonization between US and EU data rules(Christakis, 2017). This non-compliance by a major corporation like Microsoft leaves global corporations processing cross-border data requests in a state of urgent uncertainty.

c) Cybercrime Conventions: The Budapest Convention is the first international pact against cybercrime and cross-border data access, which respects national laws and sovereignty. However, in the Microsoft Ireland case, the convention's limitations in addressing cloud storage issues became apparent due to unclear dispute resolution methods.

Yahoo Data Breach (2013-2014)

a) **Mutual Legal Assistance Treaties**: MLATs impact was constrained by their limited applicability and political factors, particularly those associated with state-sponsored entities linked to Russian intelligence. These challenges lead to delays in evidence acquisition and hinder investigations, especially when evidence is spread across multiple jurisdictions, as seen in the Yahoo Breaches. Hence, the absence of an MLAT between countries and delays in MLAT processes can significantly reduce the effectiveness of these technologies, underscoring the need for improved international cooperation.

b) **Data Protection & Privacy Laws:** Yahoo's data hack raised global data protection concerns, especially regarding GDPR's cross-border data transfers. The breach exposed user account information, raising privacy concerns and new regulatory requirements. Investigators struggled to navigate European Union GDPR and US ECPA privacy laws, particularly in cloud forensics. Privacy restrictions, like user consent, hindered operations. However, the key to navigating these rules lies in finding a balance between forensic access and user privacy, as privacy restrictions can hinder forensic operations.

c) **Cybercrime Conventions:** The Budapest Convention, signed by various countries, was a key player in this arena, enabling crucial cooperation on the cybercrime investigations when breaches occur in multiple jurisdictions. Countries without such cybercrime agreements refused assistance, complicating the investigation and prosecution of culprits. Conventions also play a crucial role in governing digital evidence preservation and court presentation. Cybercrime Conventions have significantly promoted international collaboration in breach investigations, fostering law enforcement information exchange and coordination. However, their efficacy can be hampered by political will, budgetary limits, and national legal interpretations.

Uber Hack 2016

a) **Mutual Legal Assistance Treaties**: Uber's user data, likely stored across various nations, necessitated the use of Mutual Legal Assistance Treaties (MLATs) to aid in cross-border evidence collection(Ruohonen, 2023). MLATs, by enhancing collaboration, encompassing the procurement of witness testimonies, confiscating and transferring evidence, and identifying persons of interest, played a crucial role in this process. This was particularly significant as Uber's data was housed on cloud servers across many nations. MLATs were presumably employed to solicit forensic access to logs, backups, and other metadata beyond the primary investigative jurisdiction. However, challenges

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

associated with MLATs, such as protracted and bureaucratic procedures and discrepancies in legal norms among nations, also underscore the need for continuous improvement in international cooperation.

b) **Data Protection & Privacy Laws:** Uber's prolonged failure to disclose a breach for more than a year indicates substantial data protection and privacy legislation infringements(Kiesow, 2020). The General Data Protection Regulation (GDPR) and some US state regulations, including California's, mandated that Uber swiftly inform authorities and individuals. Uber's postponed disclosure contravened these regulations, highlighting the importance of timely and responsible data breach disclosure. Moreover, investigators in nations where Uber functioned must adhere to national privacy legislation during forensic inquiries, including safeguarding personally identifiable information (PII) throughout evidence preservation and processing.

c) **Cybercrime Conventions:** The Budapest Convention ensured the admissibility of evidence in courts across participating jurisdictions, instilling confidence in the integrity of international investigations. It also facilitated cooperation between countries involved in investigations, particularly in areas like sharing investigative information, preserving data, and exterminating suspects. The convention also addresses procedural and jurisdictional issues in collecting digital evidence, ensuring a harmonized approach across jurisdictions. Moreover, it sets standards for handling and analyzing evidence, similar to Uber's breach.

Facebook-Cambridge Analytica (2018)

a) **Mutual Legal Assistance Treaties**: Facebook and Cambridge Analytica, operating across multiple jurisdictions, including the United States and the United Kingdom, often stored their data in international cloud infrastructures. The procedures involved in MLATs can be lengthy and intricate, potentially slowing down investigations in the rapidly evolving digital landscape(Abraha, 2019). This situation highlighted the complexities of jurisdiction over cloud-based data, especially when data localization was ambiguous.

b) **Data Protection & Privacy Laws:** In 2018, the EU's GDPR imposed strict data processing, consent, and international data transfer regulations. This regulation was critical for Facebook because it involved EU citizens' data. However, due to the lack of comprehensive federal privacy laws in the US, Facebook faces challenges in complying with GDPR(Ward, 2022). Cambridge Analytica's unconsented data processing was assessed under the UK's Data Protection Act(Symeonidis et al., 2018). The audit examined Facebook's cloud architecture to ensure compliance with GDPR and other data storage and transfer regulations.

c) **Cybercrime Conventions:** The Budapest Convention, the principal international treaty on cybercrime, was pertinent to the Facebook-Cambridge Analytica case(Ok et al., 2025). It established a framework for global collaboration in cybercrime investigations, focusing on issues such as unlawful data access and potential infringements concerning data misuse. Nonetheless, its applicability may be constrained as not all countries were signatories. However, the role of GDPR, a key data protection regulation, was pivotal in assessing the authorized acquisition and use of data, providing a sense of reassurance about the protection of data. Cloud forensics encountered obstacles, as investigators had to verify chain-of-custody and ensure secure access to logs or metadata housed internationally.

RESULTS

The Microsoft Ireland case (2013-2018) was an important legal case that impacted the legal landscape of cross-border data access and cloud forensics. It emphasized the importance of finding a balance between law enforcement requirements, the rights of individuals to privacy, and collaboration across countries. The case revealed inconsistencies between domestic laws and international frameworks, which resulted in the U.S. CLOUD Act (2018). This act provides quicker data access while preserving local privacy rules. The decision also established a precedent for cloud providers to contest overly broad requests for data from the government,

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

which emphasizes the need to strike a careful balance between law enforcement requirements, the rights to privacy, and international collaboration. The case led to discussions about whether current legal frameworks are sufficient and whether more international collaboration is needed to handle challenges related to cross-border cloud forensics.

The Yahoo Data Breach (2013-2014) has highlighted the importance of harmonizing data protection laws. The breach exposed jurisdictional challenges for law enforcement agencies, as the data was stored and accessed across multiple jurisdictions. Data sovereignty, which varies across countries, was crucial in the investigation. The breach also led to delays in response due to legal and procedural obstacles. The global nature of Yahoo's cloud infrastructure and user base further contributed to incomplete data sharing and investigations. This breach has underscored the need to reform Multilateral Law Enforcement Treaties (MLATs) and harmonize data protection laws and cybercrime conventions to improve cloud forensic investigations.

Uber Hack (2016): The 2016 Uber breach underscored the necessity for enhanced collaboration and legislation in cloud forensic investigations. It highlighted the significance of MLATs, data protection legislation, and cybercrime treaties in transnational evidence gathering, user data confidentiality, and legal responsibility. However, the case also revealed deficiencies in current institutions, particularly regarding speed and efficiency. The complexity introduced by cloud storage further complicates the identification of evidence location. Moreover, the ever-evolving nature of data protection and cybercrime legislation necessitates that investigators stay informed. The Uber hack of 2016 served as a stark reminder of the challenges posed by cross-border data breaches, even when the company's headquarters and primary data storage are in the same country. More importantly, it underscored the critical importance of strong data security, responsible issue response, and transparency. The incident also highlighted the need for countries to collaborate and harmonize their data protection and cybersecurity regulations.

Facebook-Cambridge Analytica (2018): Facebook's global infrastructure faced a daunting task in navigating the complex landscape of data access and processing laws, often conflicting between jurisdictions like the U.S. First Amendment rights and European privacy regulations. The event resulted in substantial penalties from U.S. and U.K. regulators, but also underscored the urgent need for a unified global approach to data privacy. Investigations also brought to light deficiencies in cross-border legal frameworks, further emphasizing the importance of a cohesive strategy for data privacy. However, MLATs enabled cross-border evidence sharing, but data protection and privacy rules governing data processing and permission. Cybercrime treaties added international collaboration, but the complexity of regulation gaps and cloud forensics remained. The scandal underscored the urgent need for stronger data protection laws and regulatory scrutiny of data-sharing practices on social media platforms. This is crucial to prevent similar breaches in the future and to ensure the safety and privacy of users' personal data.

Timeline of Cross-Border High-profile Cases Selected

Table 2. Timeline of cases due to legal complexities

Case Name	Start Year	End Year
The Microsoft Ireland Case	2013	2018
Yahoo Data Breach	2013	2014
Uber Hack	2016	2016
Facebook-Cambridge Analytica	2018	2018

Theoretical Underpinnings:

Legal pluralism, a concept that acknowledges the coexistence of multiple legal systems in a social environment, such as cloud forensics, presents a complex web of national laws, international treaties, and private contractual agreements that govern investigations(Mei, 2024). This intricate landscape can lead to

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

disagreements and make it challenging to determine which laws apply and how to interpret them. Cross-border investigations further complicate matters, requiring negotiation and accommodation within these legal systems, often involving MLATs or other forms of international cooperation.

Network governance theory plays a crucial role in cloud forensics, highlighting the influence of interconnected actors on policy and practice. These actors, including government agencies, law enforcement, and cloud service providers, internet service providers, cybersecurity businesses, and international organizations, are instrumental in the success of cross-border investigations. Effective communication, cooperation, and the confidence they inspire are key to their role(Murugan & Singh, 2025).

Information control theories, particularly in the context of cloud forensics, offer valuable insights into how society manages, accesses, and shares information. In cross-border investigations, data sovereignty issues can arise when data is stored in other jurisdictions. A comprehensive understanding of these theories is essential for effective cross-border investigations(Saadallah et al., 2025).

Realist and liberal international relations theories provide insights into state interaction in cross-border probes. Realism underscores the importance of state sovereignty and national interests, while liberalism promotes cooperation and the use of international rules and institutions to solve problems(Moyo, 2024). Structured collaborations such as MLATs and other international agreements play a vital role in overcoming state sovereignty issues and reassuring the audience. Additionally, power dynamics between states can significantly impact cross-border investigations.

Transnational legal theory underscores the significant role of non-state actors in cloud forensics. It highlights the interdependence of legal systems and the urgent need for robust global legal frameworks, particularly in areas like cybercrime and cloud forensics. Concepts such as territorial jurisdiction, universal jurisdiction, and the effects doctrine were crucial in explaining international cybercrime and digital evidence norms and standards, further underlining the importance of non-state actors in this field(Qian, 2024).

Defense-in-depth theory, End-to-End Encryption Theory, Chain of Custody and Evidence Integrity, International Relations and Cooperation, Ethical and Privacy Considerations, Incident Response and Attribution, and Economic and Political Considerations are cybersecurity cryptography principles. These principles are fundamental to understanding the technical and ethical aspects of cloud forensics and international law.

Strategies for International Cooperation:

International collaboration in cloud forensic investigations is not just a necessity, but a gateway to a more efficient and successful global forensic investigative framework. The benefits of such collaboration are vast, from the establishment of multilateral agreements to the utilization of technology and automation. These strategies not only enhance cooperation but also foster a sense of optimism and motivation among stakeholders. They pave the way for the creation of international forensic standards, the development of collaborative platforms, the fortification of information sharing, the resolution of privacy and sovereignty concerns, the engagement of stakeholders, the implementation of expedited dispute resolution mechanisms, the emphasis on capacity building, the hosting of global conferences and workshops, and the promotion of awareness and advocacy.

Enhancing legal frameworks is crucial for facilitating more effective collaboration in cloud forensic investigations. Standardizing national legislation concerning cybercrime, data protection, and the admission of evidence is essential for minimizing conflicts and enhancing cooperative efforts. Enhancing and refining Mutual Legal Assistance Treaties (MLATs) and establishing standards for cross-border data access are essential for formal requests for evidence and assistance. Improving communication and collaboration requires the establishment of 24/7 contact points, which are dedicated communication channels that operate round the clock to ensure timely and efficient exchange of information, the creation of secure communication platforms, the execution of joint training and exercises, and the development of trust and capacity through the promotion

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

of transparency and accountability, the provision of technical assistance and capacity building, and the cultivation of personal relationships among law enforcement and forensic professionals from various nations.

Utilizing technology is a key aspect of cloud forensics, and it's reassuring to know that significant progress is being made in this area. This includes creating standardized forensic instruments and methodologies, using cloud-based platforms for collaborative efforts, and applying AI and machine learning to scrutinize extensive datasets and discern patterns pertinent to cross-border investigations. While reconciling national security objectives with the necessity for international collaboration presents challenges, the role of technology in this field is a beacon of hope. Explicit standards and norms are essential to tackle this matter, and the progress in technology is a testament to the potential of cloud forensics.

Safeguarding data privacy and human rights is not just a consideration, but a fundamental requirement for international investigations. It's reassuring to know that appropriate measures are being taken to avert misuse and assure adherence to applicable laws and treaties. Addressing cultural and linguistic disparities is another important aspect that can facilitate the resolution of communication obstacles and enhance international collaboration in forensic investigations. These considerations reassure us that cloud forensics is not just about solving crimes, but also about upholding ethical standards and respecting human rights.

However, promoting international collaboration in cloud forensic investigations necessitates a multifaceted approach, encompassing the establishment of multilateral agreements, the development of international forensic standards, the creation of collaborative platforms, the utilization of technology and automation, the enhancement of awareness and advocacy, and the resolution of challenges and concerns. We can advance towards a more efficient and successful global forensic investigative framework by employing these tactics.

DISCUSSION

Scenario I: The Microsoft Ireland case (2013-2018)

A drug trafficking investigation in US compels Microsoft to reveal emails relevant to the investigation from a server hosted by Microsoft a US company, in Ireland. Investigators in the U.S. need to access emails stored in the Irish data center.

Data Points for Analysis:

A. **Jurisdiction:**

- **Service provider Jurisdiction:** United States
- **Requesting Jurisdiction:** United States
- **Location of the data:** Ireland (EU).

B. **Legal Frameworks:**

- **U.S. Laws:** Stored Communications Act (SCA), Clarifying Lawful Overseas Use of Data Act (CLOUD) Act.
- **EU Laws:** General Data Protection Regulation (GDPR),
- **International Treaties:** Budapest Convention on Cybercrime, Mutual Legal Assistance Treaties (MLATs) between the U.S. and Ireland.

C. **Data Types:**

- Email

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

Analysis and Evaluation:

A. Jurisdiction:

- **Complexity:** The cross-border nature of the incident creates jurisdictional challenges. Both the U.S. and Ireland could assert jurisdiction based on **the requesting jurisdiction** and **the location of the server**, respectively.

- **Evaluation:** Determining the appropriate jurisdiction(s) is crucial for establishing the applicable laws and procedures. This might require coordination between law enforcement agencies in both countries.

B. Legal Frameworks:

a) Complexity: Multiple and potentially conflicting legal frameworks apply.

- U.S. laws like the CFAA and SCA govern access to electronic communications and stored data, but their extraterritorial reach can be limited. However, the emergence of CLOUD Act in 2018 broke the complexity with US cloud service providers.

- The GDPR imposes strict requirements for processing personal data of EU citizens, even if the data is processed outside the EU.

- The Budapest Convention provides a framework for international cooperation in cybercrime investigations, but its effectiveness depends on the extent of its implementation in each country.

- MLATs can facilitate the exchange of evidence between countries, but the process can be slow and complex.

b) Evaluation: Investigators navigate these complex legal frameworks to ensure that their actions are lawful in all relevant jurisdictions. This involved obtaining warrants or other legal authorizations in both the U.S. and Ireland.

C. Data Types:

a) Complexity: The type of data being sought affected the applicable legal requirements.

1. In this case the data required here were **emails** which is subject to the CFAA and SCA which govern access to electronic communications and stored data, and CLOUD Act.

2. The GDPR imposes specific obligations for handling personal data, including requirements for data minimization, purpose limitation, and data security.

b) Evaluation: Investigators must carefully consider the type of data they need and ensure that they have a valid legal basis for accessing it. If personal data is involved, they must comply with the GDPR and other applicable data protection laws.

Practical Demonstration of Analysis:

Let's focus on the GDPR aspect.

A. **Analysis:** Since the data type is email, it is considered personal data under the GDPR. This means that U.S. investigators would need to demonstrate a valid legal basis for processing this data, such as:

1) Consent from the data subjects.

2) Necessity for the performance of a contract.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

3) Compliance with a legal obligation.

4) Protection of vital interests.

5) Performance of a task carried out in the public interest.

6) Legitimate interests pursued by the controller or a third party.

B. **Evaluation:** In this situation, it is improbable that investigators in the United States could depend on consent or a contract. They may claim that processing the data is required to comply with a legal requirement to protect legitimate interests, such as the crucial task of preventing additional harm. This claim would need to be thoroughly evaluated, considering the GDPR's standards for proportionality and necessity.

CONCLUSION

This Microsoft Ireland scenario vividly illustrates the legal complexities of cross-border cloud forensic investigations. Investigators, including legal professionals, data protection officers, and IT security experts, must navigate a complex web of national laws, international treaties, and data protection regulations. Your careful analysis and evaluation of the relevant legal frameworks, data types, and jurisdictional issues are essential for ensuring that investigations are conducted lawfully and effectively. The case highlighted the urgent need for international agreements to address cross-border data access, leading to discussions on bilateral data-sharing agreements under the CLOUD Act. It set a precedent for balancing data privacy, territorial sovereignty, and law enforcement and warned global tech companies about the potential reach of their home country's laws.

Yahoo Data Breach Scenario II:

Scenario 1:

A data breach originates from a server hosted by a cloud provider Yahoo in the US. The main issue is Cybercrime; unauthorized access to computer systems and theft of data.

Data Points for Analysis:

1. **Jurisdiction:**

a) **Location of the crime:** Potentially the U.S. (where the victims are located) and China (where the server is located).

b) **Location of the data:** US and Others

c) **Nationality of victims:** Potentially U.S.

2. **Legal Frameworks:**

a) **U.S. Laws:** International Emergency Economic Powers Act (IEEPA), the Foreign Investment Risk Review Modernization Act (FIRRMA)

b) **EU Laws:** General Data Protection Regulation (GDPR)

c) **China:** Data Security Law (DSL) and Cybersecurity Law.

d) **International Treaties:** Budapest Convention on Cybercrime,

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

3. **Data Types:**

a) Potentially personal data and sensitive information of US citizens.

Analysis and Evaluation:

1. Jurisdiction:

A. **Complexity:** The cross-border nature of the incident creates jurisdictional challenges. Both the U.S. and China could assert jurisdiction based on the location of the victim and the location of the server, respectively.

B. **Evaluation:** Determining the appropriate jurisdiction(s) is crucial for establishing the applicable laws and procedures. This might require coordination between law enforcement agencies in both countries.

2. Legal Frameworks:

A. **Complexity:** Multiple and potentially conflicting legal frameworks apply.

1) U.S. laws like the International Emergency Economic Powers Act (IEEPA), the Foreign Investment Risk Review Modernization Act (FIRRMA) but their extraterritorial reach could be limited.

2) The GDPR imposed strict requirements for processing personal data of EU citizens, even if the data is processed outside the EU.

3) The Budapest Convention provided a framework for international cooperation in cybercrime investigations, but its effectiveness depends on the extent of its implementation in each of the countries.

B. **Evaluation:** Investigators navigated these complex legal frameworks to ensure that their actions were lawful in all relevant jurisdictions. This involved obtaining warrants or other legal authorizations in both the U.S. and Other Countries.

3. Data Types:

A. **Complexity:** The type of data being sought affects the applicable legal requirements.

1) In this case the data required here were personal data and sensitive information of US citizens which is subject to the CFAA and SCA which govern access to electronic communications and stored data.

2) The GDPR imposes specific obligations for handling personal data, including requirements for data minimization, purpose limitation, and data security.

B. **Evaluation:** Investigators must carefully consider the type of data they need and ensure that they have a valid legal basis for accessing it. If personal data is involved, they must comply with the GDPR and other applicable data protection laws.

Practical Demonstration of Analysis:

Let's focus on the GDPR aspect.

A. **Analysis:** If the server contains personal data and sensitive information of US citizens, this could be considered personal data under the GDPR. This means that U.S. investigators would need to demonstrate a valid legal basis for processing this data, such as:

Consent from the data subjects.

1) Necessity for the performance of a contract.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

2) Compliance with a legal obligation.

3) Protection of vital interests.

4) Performance of a task carried out in the public interest.

5) Legitimate interests pursued by the controller or a third party.

B. **Evaluation:** It is unlikely that U.S. investigators could rely on consent or a contract in this scenario. They might argue that processing the data is not just necessary, but crucial to comply with a legal obligation (e.g., investigating a cybercrime) or to prevent further harm. However, this argument must be meticulously assessed in light of the GDPR's requirements for proportionality and necessity.

Conclusion

The Tiktok Data Concern scenario serves as a stark reminder of the legal intricacies involved in cross-border cloud forensic investigations. It underscores the responsibility of investigators to meticulously study and appraise the relevant national laws, international conventions, and data protection rules. The successful and legal execution of investigations is a testament to the diligence and responsibility of the investigators in understanding the pertinent legal frameworks, data types, and jurisdictional concerns.

Lesson learned:

Early legal consultation is crucial for investigators in cross-border investigations, ensuring effective collaboration between law enforcement agencies. International cooperation is also essential, as effective investigations require strong cooperation across different countries. Data protection and privacy must be respected, including GDPR.

Comparative Analysis:

Cloud forensic investigations in cross-border situations require navigating a complicated network of legal frameworks and procedures that differ from one jurisdiction to another. This intricacy can make it challenging to gather and use digital evidence. However, investigators can enhance the efficiency and efficacy of their investigations by recognizing common difficulties and best practices.

The Stored Communications Act (SCA), the Computer Fraud and Abuse Act (CFAA), the Electronic Communications Privacy Act (ECPA), the General Data Protection Regulation (GDPR), the ePrivacy Directive, and international treaties such as the Budapest Convention on Cybercrime and Mutual Legal Assistance Treaties (MLATs) are all important legal frameworks that are relevant to cloud forensic investigations. There are significant variances in data protection standards, access to data, international collaboration, jurisdictional concerns, data protection laws, acquiring evidence, technical challenges, and early legal advice.

When conducting cloud forensic investigations in cross-border contexts, seeking legal advice early on is not just crucial, it's a cornerstone of the investigation. This early legal advice provides a solid foundation for the investigation and reassures the investigators about the legality of their actions. Cooperating with foreign partners, minimizing data collection, having technical knowledge, and following established methods are all important. It is essential to consult with legal professionals in all relevant jurisdictions early in the inquiry. Creating clear communication lines and cooperating with law enforcement officials in other nations is also important. Hiring investigators with knowledge of cloud forensics and related technologies is essential to overcome technical hurdles. Standardized methods for gathering, storing, and analyzing data can ensure evidence is accepted in multiple jurisdictions.

Common obstacles in cloud forensic investigations include jurisdictional issues, MLAT inefficiencies, data localization, provider-specific challenges, and evidence admissibility. However, these difficulties can be

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

effectively addressed through international cooperation, standardization, and partnerships. By emphasizing the role of international cooperation in overcoming these obstacles, the audience will feel the importance of collaboration in their work.

The Stored Communications Act (SCA) and the Computer Fraud and Abuse Act (CFAA) regulate access to electronic evidence in the United States, the European Union, and the Asia-Pacific area. The General Data Protection Regulation (GDPR) establishes severe requirements for data protection and the ePrivacy Directive. When governments, cloud providers, and forensic experts work together in public-private partnerships, they can make procedures more efficient and settle jurisdictional disputes. Training and awareness training can help improve efficacy in situations that involve multiple countries.

However, the United States, the European Union, and the Asia-Pacific area have different cloud forensics methods. However, they also face similar issues, such as jurisdictional conflicts, inefficiencies in the mutual legal assistance treaty (MLAT), and data localization. Best practices highlight the importance of international cooperation, standardization, and partnerships to tackle these difficulties effectively. By reiterating the importance of these strategies, this will help establish a cohesive and efficient framework for cross-border cloud forensic investigations, making the audience feel the significance of their work.

POLICY RECOMMENDATIONS

This study suggests ways to enhance legal frameworks and create new laws to facilitate cloud forensic investigations across borders. These include harmonizing data sovereignty laws, streamlining Mutual Legal Assistance Treaties (MLATs), enhancing data privacy regulations, establishing international standards, addressing technical challenges such as data encryption and jurisdictional issues, fostering international cooperation, and continuously reviewing and adapting legal frameworks and policies to keep pace with the dynamic nature of technology and data privacy.

1. Data sovereignty regulations can be harmonized by creating international agreements that establish explicit data ownership, control, and access norms in the cloud environment. This will streamline cross-border investigations, enhance efficiency, and provide clarity in data management.

2. The urgency of updating MLATs to effectively deal with digital evidence and cloud computing issues cannot be overstated. This includes creating specific channels for urgent requests and encouraging the use of technology-enabled platforms for safe data exchange across borders, highlighting the need for immediate action.

3. Improving data privacy regulations by creating clear rules for accessing and sharing data, protecting privacy rights, and encouraging the use of privacy-enhancing technologies is of utmost importance. This not only reassures individuals about the safety of their data but also provides a strong legal framework for investigations, instilling a sense of security and confidence.

4. Establish worldwide standards and best practices for cloud forensic investigations, such as creating a global certification body or developing a set of universally accepted procedures, and encourage using standardized techniques and technology.

5. Encourage cloud service providers to establish strong security measures, such as robust data encryption and regular security audits, and develop powerful forensic tools, like advanced data recovery systems and real-time monitoring solutions, to address technical issues in cloud systems.

6. Promote international cooperation by enhancing engagement between law enforcement agencies and legal experts, creating collaborative training programs, and encouraging using technology-enabled platforms for secure communication and collaboration.

However, unified legislation and cooperation across various cross-border jurisdictions and authorities can help resolve cross-border issues. As a result, it is critical not to overestimate the importance of cultural and communication differences while promoting international cooperation. To manage effectively, it is vital to be

aware of these disparities and proactively use measures to bridge communication gaps. This technique, engaging local experts and understanding area practices, is key to a deeper understanding of the legal complexities of cloud forensics investigations and cross-border cooperation.

REFERENCES

1. Abraha, H. H. (2019). How compatible is the US 'CLOUD Act' with cloud computing? A brief analysis. International Data Privacy Law, 9(3), 207–215. https://doi.org/10.1093/idpl/ipz009
2. AllahRakha, N. (2024). Demystifying the Network and Cloud Forensics' Legal, Ethical, and Practical Considerations. Pakistan Journal of Criminology, 16.2, 119–132. https://doi.org/10.62271/pjc.16.2.119.132
3. Alshabibi, M. M., Bu dookhi, A. K., & Hafizur Rahman, M. M. (2024). Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review. Computers, 13(8), Article 8. https://doi.org/10.3390/computers13080213
4. Annas, W., Malik, David, S., Bhatti, Tae-Jin, P., Hafiz, U., Ishtiaq, Jae-Cheol, R., & Ki-Il, K. (2024). Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges. Https://Doi.Org/10.3390/S24020433. https://www.mdpi.com/1424-8220/24/2/433
5. Ashurov, A. (2024). Jurisdictional Challenges in Cross-Border Cybercrime Investigations. Центральноазиатский журнал междисциплинарных исследований и исследований в области управления, 1(8), Article 8. https://www.in-academy.uz/index.php/cajmrms/article/view/31783
6. Böhm, H. (2021). Five Roles of Cross-border Cooperation Against Re-bordering: Journal of Borderlands Studies: Vol 38, No 3. https://www.tandfonline.com/doi/abs/10.1080/08865655.2021.1948900
7. Brown, G., & Peterson, R. S. (2022). The Distended Board: Uber. In G. Brown & R. S. Peterson (Eds.), Disaster in the Boardroom: Six Dysfunctions Everyone Should Understand (pp. 113–124). Springer International Publishing. https://doi.org/10.1007/978-3-030-91658-9_7
8. Buçaj, E., & Idrizaj, K. (2025). The need for cybercrime regulation on a global scale by the international law and cyber convention. Multidisciplinary Reviews, 8(1), 2025024–2025024. https://doi.org/10.31893/multirev.2025024
9. Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: Cross-border criminal investigations and digital evidence. Journal of Cybersecurity, 8(1), tyac014. https://doi.org/10.1093/cybsec/tyac014
10. Christakis, T. (2017). Data, Extraterritoriality and International Solutions to Transatlantic Problems of Access to Digital Evidence. Legal Opinion on the Microsoft Ireland Case (Supreme Court of the United States) (SSRN Scholarly Paper No. 3086820). Social Science Research Network. https://papers.ssrn.com/abstract=3086820
11. Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A., & Sheikh, A. (2011). The case study approach. BMC Medical Research Methodology, 11, 100. https://doi.org/10.1186/1471-2288-11-100
12. Currie, R. J. (2017). Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "Next Frontier"? Canadian Yearbook of International Law/Annuaire Canadien de Droit International, 54, 63–97. https://doi.org/10.1017/cyl.2017.7
13. Deandra, F., Hafiz, & Sherly, I., Muda. (2025). ADVANCING DIGITAL FORENSIC INVESTIGATIONS: ADDRESSING CHALLENGES AND ENHANCING CYBERCRIME SOLUTIONS. World Journal of Information Technology, 3(1). https://doi.org/10.61784/wjit3018
14. Dickson, D. J. (2024). The European Arrest Warrant in Scots Law. Transnational Criminal Law Review, 3(1), Article 1. https://doi.org/10.22329/tclr.v3i1.8495
15. Egho-Promise, E., Idahosa, S., Asante, G., & Okungbowa, A. (2024). Digital Forensic Investigation Standards in Cloud Computing. Universal Journal of Computer Sciences and Communications, 23–45. https://www.scipublications.com/journal/index.php/ujcsc/article/view/923
16. Enhancing Trust and Immutability in Cloud Forensics | SpringerLink. (n.d.). Retrieved October 7, 2024, from https://link.springer.com/chapter/10.1007/978-981-15-8289-9_74
17. Forensics framework for cloud computing—ScienceDirect. (n.d.). Retrieved October 11, 2024, from https://www.sciencedirect.com/science/article/abs/pii/S0045790617302689?via%3Dihub

18. Gruber, A., & Robin Pierce, J. D. (2019). Transatlantic challenges in access to electronic evidence: Conflicting obligations under the Stored Communications Act and the General Data Protection Regulation. https://arno.uvt.nl/show.cgi?fid=148179
19. Hazlett, T. W. (2023). Populist Antitrust: The Case of FTC v. Facebook. The Antitrust Bulletin, 68(2), 250–262. https://doi.org/10.1177/0003603X231163218
20. Islam, Md. T., & Karim, R. (2022). Cybersecurity and Integrated Business Models. In S. Singh Dadwal, H. Jahankhani, & A. Hassan (Eds.), Integrated Business Models in the Digital Age: Principles and Practices of Technology Empowered Strategies (pp. 3–46). Springer International Publishing. https://doi.org/10.1007/978-3-030-97877-8_1
21. Jerman-Blažič, B. & Tomaž Klobučar. (2020). A New Legal Framework for Cross-Border Data Collection in Crime Investigation amongst Selected European Countries. https://doi.org/10.5281/ZENODO.3698359
22. Jougleux, P. (2022). Personal Data and Privacy Protection: Facebook and the Big Data Mountain. In P. Jougleux (Ed.), Facebook and the (EU) Law: How the Social Network Reshaped the Legal Framework (pp. 13–92). Springer International Publishing. https://doi.org/10.1007/978-3-031-06596-5_2
23. Kiesow, C., Elif. (2020). Data Breaches and GDPR | SpringerLink. https://link.springer.com/referenceworkentry/10.1007/978-3-319-78440-3_39
24. Lemieux, F. (2024). National and Transnational Police Cooperation. In Intelligence and State Surveillance in Modern Societies (pp. 105–114). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83549-097-620242006
25. Machova, T. (2021). The discourse of surveillance and privacy: Biopower and panopticon in the Facebook-Cambridge Analytica scandal. https://urn.kb.se/resolve?urn=urn:nbn:se:mau:diva-44664
26. Malik, A. W., Bhatti, D. S., Park, T.-J., Ishtiaq, H. U., Ryou, J.-C., & Kim, K.-I. (2024). Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges. Sensors, 24(2), Article 2. https://doi.org/10.3390/s24020433
27. McGovern, V. (2024). Uber: Cyber Breaches. SAGE Publications: SAGE Business Cases Originals. https://doi.org/10.4135/9781071939994
28. Mei, M. D. M. (2024). KIGALI INDEPENDENT UNIVERSITY ULK SCHOOL OF LAW DEPARTMENT OF LAW P.O BOX 2289 KIGALI.
29. Michels, J. D., Millard, C., & Walden, I. (2023). On Cloud Sovereignty: Should European Policy Favour European Clouds? (SSRN Scholarly Paper No. 4619918). Social Science Research Network. https://doi.org/10.2139/ssrn.4619918
30. Moyo, I. (2024). Cross Border Security in the Southern African Region: Transcending Statolatry. Taylor & Francis.
31. Murugan, T., & Singh, W. J. (2025). Cybersecurity and Data Science Innovations for Sustainable Development of HEICC: Healthcare, Education, Industry, Cities, and Communities. CRC Press.
32. Nelufule, N., Masango, M., & Singano, T. (2024). The Future of Digital Forensic Investigations: Keeping the Pace with Technological Advancements. 2024 47th MIPRO ICT and Electronics Convention (MIPRO), 1843–1848. https://doi.org/10.1109/MIPRO60963.2024.10569461
33. Ok, E., Aria, J., Jose, D., & Diego, C. (2025). The Impact of Cybersecurity Laws on Legal Procedures and Case Law.
34. Olber, P. (2021). The survey on cross-border collection of digital evidence by representatives from Polish prosecutors' offices and judicial authorities. Journal of Digital Forensics, Security and Law, 16(2). https://doi.org/10.58940/1558-7223.1700
35. Ozioko, A. C. (2024). Legal Challenges in Digital Forensics for Financial Crime Investigations. Global Research for New World Order, 5(1), Article 1. http://journals.frankridgeconsortium.com/index.php/GRNWO/article/view/49
36. Patterson, A. (2020). The Ongoing Issue of Cyber Insecurity: Why Cyber Insurance Should Be Mandatory for Consumer Companies. Florida State University Law Review, 48, 841. https://heinonline.org/HOL/Page?handle=hein.journals/flsulr48&id=889&div=&collection=
37. Qian, X. (2024). Redefining International Law Paradigms: Charting Cybersecurity, Trade, and Investment Trajectories within Global Legal Boundaries in: The Journal of World Investment & Trade Volume 25 Issue 3 (2024). https://brill.com/view/journals/jwit/25/3/article-p295_1.xml

38. Robbins, J. M., & Sechooler, A. M. (2018). Once More unto the Breach: What the Equifax and Uber Data Breaches Reveal about the Intersection of Information Security and the Enforcement of Securities Laws. Criminal Justice, 33, 4. https://heinonline.org/HOL/Page?handle=hein.journals/cjust33&id=6&div=&collection=
39. Ruohonen, J. (2023). Recent Trends in Cross-Border Data Access by Law Enforcement Agencies (No. arXiv:2302.09942). arXiv. https://doi.org/10.48550/arXiv.2302.09942
40. Saadallah, M., Shahim, A., & Khapova, S. (2025). Harmonizing Paradoxical Tensions in SOCs: A Strategic Model for Integrating AI, Automation, and Human Expertise in Cyber Defense and Incident Response. https://hdl.handle.net/10125/109586
41. Safie, S. I., & Bin Md Bashah, S. R. (2024). Implementing ISO 27037 for Digital Forensics in the Malaysian Anti-Corruption Commission: Challenges and Solutions. 2024 IEEE 10th International Conference on Smart Instrumentation, Measurement and Applications (ICSIMA), 81–85. https://doi.org/10.1109/ICSIMA62563.2024.10675543
42. Sargiotis, D. (2024). Data Governance Frameworks: Models and Best Practices. In D. Sargiotis (Ed.), Data Governance: A Guide (pp. 165–195). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-67268-2_4
43. Sharma, S. (2020). Issues with enforcing Mutual Legal Assistance Treaties (MLATs): Access to cross-border data in criminal investigation (SSRN Scholarly Paper No. 3815270). Social Science Research Network. https://doi.org/10.2139/ssrn.3815270
44. Sibe, R. T., & Kaunert, C. (2024). Digital Evidence, Digital Forensics, and Digital Forensic Readiness. In R. T. Sibe & C. Kaunert (Eds.), Cybercrime, Digital Forensic Readiness, and Financial Crime Investigation in Nigeria (pp. 57–83). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-54089-9_3
45. Syaakirah, C., Rafifah, Syifa, L., & Muda, I. (2025). DIGITAL FORENSIC INVESTIGATION IN CYBERCRIME CASES: CASE STUDIES AND RECOMMENDATIONS. Multidisciplinary Journal of Engineering and Technology, 2(1). https://doi.org/10.61784/mjet3018
46. Symeonidis, I., Biczók, G., Shirazi, F., Pérez-Solà, C., Schroers, J., & Preneel, B. (2018). Collateral damage of Facebook third-party applications: A comprehensive study. Computers & Security, 77, 179–208. https://doi.org/10.1016/j.cose.2018.03.015
47. Toussaint, M., Krima, S., & Panetto, H. (2024). Industry 4.0 data security: A cybersecurity frameworks review. Journal of Industrial Information Integration, 39, 100604. https://doi.org/10.1016/j.jii.2024.100604
48. Trautman, L. J., & Ormerod, P. C. (2016). Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach. American University Law Review, 66, 1231. https://heinonline.org/HOL/Page?handle=hein.journals/aulr66&id=1275&div=&collection=
49. Tréguer, F. (2018). US Technology Companies and State Surveillance in the Post-Snowden Context: Between Cooperation and Resistance.
50. Tripathi, M., & Mukhopadhyay, A. (2022). Does privacy breach affect firm performance? An analysis incorporating event-induced changes and event clustering. Information & Management, 59(8), 103707. https://doi.org/10.1016/j.im.2022.103707
51. Tyagi, A. K., Dananjayan, S., Agarwal, D., & Thariq Ahmed, H. F. (2023). Blockchain—Internet of Things Applications: Opportunities and Challenges for Industry 4.0 and Society 5.0. https://www.mdpi.com/1424-8220/23/2/947
52. Verma, A., Jawanda, K., & Kaur, A. (2021). Data Privacy and Cambridge Analytica: A Case Study. Supremo Amicus, 24, [368]. https://heinonline.org/HOL/Page?handle=hein.journals/supami24&id=368&div=&collection=
53. Vogt, S. D. (2017). The Digital Underworld: Combating Crime on the Dark Web in the Modern Era. Santa Clara Journal of International Law, 15, 104. https://heinonline.org/HOL/Page?handle=hein.journals/scjil15&id=104&div=&collection=
54. Ward, A. (2022). The Oldest Trick in the Facebook: Would the General Data Protection Regulation Have Stopped the Cambridge Analytica Scandal? Trinity College Law Review, 25, 221. https://heinonline.org/HOL/Page?handle=hein.journals/trinclr25&id=229&div=&collection=

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue I January 2026

55. Zhang, H., & Gong, X. (2024). The research on an electronic evidence forensic system for cross-border cybercrime. The International Journal of Evidence & Proof, 28(1), 21–44. https://doi.org/10.1177/13657127231187059
56. Zuo, Z. (2024). Cross-Border Data Forensics: Challenges and Strategies in the Belt and Road Initiative Digital Era. Asian Social Science, 20(2), Article 2. https://doi.org/10.5539/ass.v20n2p49