# A Privacy-Compliant Process for Digital Forensics Readiness

**Gabriel Shoderu, Stacey Baror and Hein Venter**
University of Pretoria, South Africa

go.shoderu@gmail.com
stacey.baror@up.ac.za
hein.venter@up.ac.za

**Abstract:** This research paper examines the issue of privacy compliance in digital forensics readiness, specifically in relation to the breach of confidentiality during analysis of collected data on users. This is a problem because the collection and analysis of digital evidence during these investigations can have a potential impact on individuals' privacy rights. The study's methodology involves a literature review of relevant research, an analysis of privacy regulations, and a case study of a real-world digital forensics investigation. The main findings of the study indicate that organizations need to develop and implement robust privacy measures and data protection policies to ensure that their digital forensics readiness efforts are privacy compliant and do not compromise user privacy. Some examples of why this is necessary are provided in the research to address these privacy compliance issues, this study proposes a measure, this measure implements technical safeguards to protect user data and maintains its confidentiality. By implementing the proposed measures, organizations can maintain their digital forensics readiness while also protecting user privacy.

**Keywords:** Digital forensics readiness, Information privacy, Digital forensics investigation, Confidentiality, Digital forensics

## 1. Introduction

In today's digital age, cybercrime has become increasingly rampant and complex (Anderson *et al.*, 2019), posing significant threats to individuals, businesses, and organizations. To combat such criminal activities, digital investigative techniques are widely used to track and identify suspects. However, as the volume and severity of cybercrime continue to escalate, so do the challenges associated with conducting digital forensics investigations while maintaining privacy and data protection. One innovative solution to this problem is the development of digital forensic readiness which was first introduced by Tan (Tan, 2001), which takes a proactive approach to identifying and addressing digital evidence before any criminal activity occurs. This approach involves implementing policies, procedures, and technologies to facilitate the timely collection, preservation, and analysis of digital evidence in a way that is both effective and privacy compliant. Despite the many benefits of digital forensics readiness, there are still privacy concerns to be addressed (Yaacoub *et al.*, 2021; Anon, n.d.). These concerns centre on issues such as the collection and use of personal data, the retention and storage of digital evidence, and the potential for abuse of investigative powers. As such, any digital forensics readiness process must be designed and implemented with careful consideration of privacy and data protection regulations, ensuring that the rights and freedoms of individuals are respected and protected throughout the investigative process. Although digital forensics readiness ensures the quality and availability of evidence, it also involves collecting evidence in advance of a crime, which can be used to prosecute suspects anytime.

However, the problem is that the collection and analysis of digital evidence during these investigations can have a potential impact on individuals' privacy rights. For example, an organization investigates an employee for theft of confidential information, releases information to the media and employees, damaging the employee's reputation. The investigation clears the employee of all charges, but the damage is already done, and the information that was released about them cannot be taken back. The employee may face difficulty regaining the trust of their colleagues, clients, and competitors, and their career prospects may be negatively impacted. Therefore, this study aims to create a model that enhances the digital forensics readiness process in such a way that it is privacy compliant, while still maintaining the necessary level of investigative rigor.

The breach of confidentiality can lead to ethical concerns, as users have a right to privacy and expect their personal information to be always protected. The breach of confidentiality of user information can result in a damaged reputation of an organization, as users may lose the trust in their ability to protect their personal information. It may lead to non-compliance with privacy laws and could lead to financial penalties for organizations. In addition, collecting and analysing user information during digital forensics investigations can violate individuals' privacy rights, especially if sensitive or personal data is involved. This can be illegal under some acts and regulations in certain countries, such as the POPIA act. It is important that organizations have measures in place to protect user privacy, while still maintaining the necessary level of digital forensics readiness to detect, respond to, and investigate digital incidents.

This initial section, Section 1, serves as an introductory segment, setting the stage by defining the research problem and outlining the motivation behind the study. Subsequently, Section 2 delves into the background, providing essential context on digital forensic readiness and the regulatory framework surrounding user privacy. In Section 3, a model is developed, incorporating the most pertinent practices and techniques identified during the literature review. Section 4 introduces a comprehensive case scenario. The research further reviews related literature in Section 5, comparing the work of other authors with the proposed model. Finally, Section 6, the conclusion, provides a summative overview of the research and its contributions, offering insightful recommendations for future investigations in this field. The subsequent section delves deeper into the background literature.

## 2. Background Literature

This section delves deeper into the relevant literature on digital forensics to provide a more comprehensive understanding of the challenges and opportunities in this field and a background on user privacy regulations.

### 2.1 Background on Digital Forensics

The field of forensics initially focused on traditional forms of evidence collection and analysis such as fingerprints, DNA, and other physical evidence. As technology evolved and became more integrated into our daily lives, digital devices and systems started to play a more significant role in criminal investigations. This led to the emergence of computer forensics as a specialized field within forensics that dealt specifically with digital devices and systems such as personal computers. According to Daniel (Daniel and Daniel, 2011), digital forensics originated from computer forensics, which initially focused on personal computers. However, as the scope of computer forensics expanded to encompass various fields and practices, the term became limited. Thus, the term digital forensics was adopted to reflect the broader range of devices and systems that require forensic investigation.

Digital forensics is a branch of forensic science (Andre, 2018), that uses a scientifically derived and proven methods towards a distinct and definite process of deriving digital evidence from a digital source. The purpose of following these distinct processes is to facilitate or further the reconstruction of events as a result of criminal or non-criminal action. These processes are preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation(Hein Venter, n.d.) This field encompasses multiple disciplines (Omeleze and Venter, n.d.; Hein Venter, n.d.), including computer science, cybersecurity, information security, conventional forensics, law, ethics and more. Computer science plays a crucial role in digital forensics, as both cybersecurity and forensics are built on computer-related concepts. While forensics is a subset of cybersecurity, it can also stand alone and be intertwined with cybersecurity. It also involves various fields including criminalistics, pathology, odontology, entomology and many more. (Rowlingson, 2004; Hein Venter, n.d.)

These various disciplines and fields must work together in order to uncover and analyse evidence through investigation. By utilizing a multidisciplinary approach, digital forensics can uncover evidence that may be hidden or difficult to find and use that evidence in legal proceedings. This uncovered evidence must be accurate, admissible, authentic, complete, reliable, believable and verifiable. (H. S. Venter, n.d.)

Digital forensic investigations typically focus on gathering evidence after the decision to initiate an investigation. However, the success of a digital forensics investigation relies on the availability and discovery of relevant evidence. If the necessary evidence exists and is located during the investigation, it can be used in charging and prosecuting a suspect. If the required evidence does not exist, it may impede the ability to press charges and carry out prosecution. This is where DFR comes in (HS Venter, n.d.), DFR attempts to gather the necessary evidence before an incident takes place in a bid to have more sound evidence when an investigation needs to take place, the formal definition is given by Rowlingson.

According to Rowlingson (Rowlingson, 2004), Digital forensic readiness is the ability of an organization to maximise its potential to use digital evidence whilst minimising the costs of an investigation. There are two main objectives of digital forensic readiness (HS Venter, n.d.), they are to:

- Maximize an environment's ability to collect credible digital evidence.
- Minimize the cost of forensics during an incident response.

The foundational DFR processes delineated by ISO IEC 27043 encompass five process classes, readiness process, initialization process, acquisitive process, investigative process and concurrent process, the fifth being executed concurrently. All these processes work together in order to fulfil the objectives stated above.

The following section delves deeper into what privacy is, what the regulation behind privacy is, techniques to address privacy.

### 2.2 Background on Information Privacy

#### *2.2.1 Information privacy*

Information privacy pertains to the right of individuals to exercise control over the collection, use, and dissemination of their personal information. Pavlou (Paul A. Pavlou, 2011) describes it as the concept of regulating the acquisition and utilization of one's personal information. Information privacy is heavily regulated by laws and regulations as discussed in the next section, one very specific regulation in the south African context is the Protection of Personal Information Act (POPIA) regulation.

POPIA is a significant regulatory framework that has a direct impact on digital forensic investigations involving personal information. POPIA aims to safeguard the privacy and protection of personal data in South Africa. (South African Government Gazette., n.d.)

Under POPIA, organizations are required to comply with certain principles and obligations when collecting, processing, and storing personal information. These principles include accountability, purpose specification, data minimization, accuracy, security safeguards, and data subject participation.

In the context of digital forensic investigations, the provisions of POPIA impose additional considerations and limitations on the collection, analysis, and storage of personal information. Investigators must adhere to the principles of lawfulness, fairness, and transparency when handling personal data. They should ensure that the collection of personal information is justified, limited to the purpose of the investigation, and conducted with the necessary consent or legal basis.

Furthermore, POPIA grants data subjects certain rights, such as the right to access their personal information, request its correction or deletion, and object to its processing. These rights may impact the procedures and practices followed during digital forensic investigations, requiring investigators to handle personal data in a manner that respects the rights of individuals. By incorporating the principles and provisions of POPIA into digital forensic investigations, organizations can ensure a privacy-compliant approach while preserving the integrity and admissibility of digital evidence.

In this research we will be making use of block-chain technology (Mohanta *et al.*, 2019) to enforce privacy, the following subsection sheds some lights on blockchain technology.

#### *2.2.2 Blockchain Technology And Information Privacy*

Blockchain technology offers an enticing solution for enhancing information privacy, particularly in digital forensic investigations. It serves as a decentralized, tamper-resistant ledger for securely recording data. (Mohanta *et al.*, 2019; Nakamoto, n.d.). Each data entry forms an immutable link in a chain, making it resistant to alterations—ideal for safeguarding sensitive information and Digital Forensic Readiness (DFR).

In the realm of information privacy, blockchain's decentralized structure encrypts and disperses personal data across multiple network nodes, reducing data breach risks. Additionally, blockchain enhances data transparency and accountability through smart contracts and consensus mechanisms, allowing individuals greater control over their data(Paul A Pavlou, 2011).

In summary, blockchain's security, transparency, and accountability have the potential to revolutionize information privacy within digital forensics, enabling organizations to align with privacy regulations while enhancing digital forensic practices. The subsequent sections detail our conceptual model and its components, providing a roadmap for privacy-compliant digital forensics readiness.

## 3. High Level View of BlockTrace Model

This section presents a holistic model aimed to seamlessly integrate the DFR processes with robust privacy standards, thereby creating a new phase of investigative readiness and adherence, we call this model, the BlockTrace model.

As this section progresses, the primary concern is attempting to harmonize digital forensics investigations with privacy standards. This model emerges as a direct response to the pressing need to not only enhance DFR but also ensure that every investigative action adheres to privacy principles.

The journey is started with a detailed breakdown of the proposed model and its respective components. Built upon the solid grounds of information privacy principles, the model aims to harmonize investigative efficiency with the protection of individuals' privacy rights.

As we delve into this section, we will exclusively explore these novel components and their profound impact on improving DFR processes while upholding the highest standards of privacy protection.

Commencing with the higher-level view of the BlockTrace model as shown in Figure 1, we embark on an exploration of each component we contribute, beginning with the overview of the Privacy initialization process (PIP), labelled B followed by the Privacy check process, labelled F.

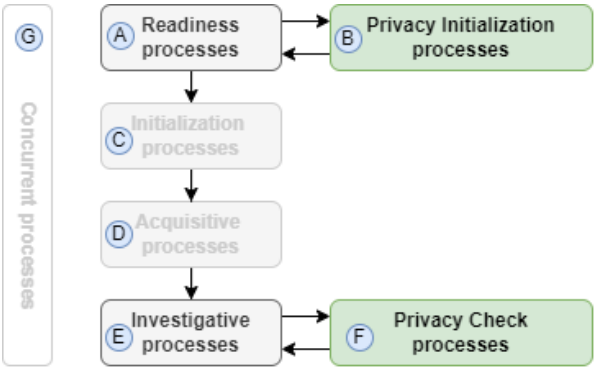


**Figure 1: Adapting ISO/IEC 27043 (Labelled High-level view of BlockTrace Model)**

### 3.1 Privacy Initialization Process (PIP)

The Privacy Initialization Process (PIP), a pioneering addition to the traditional DFR processes, represents a pivotal step towards integrating privacy-conscious practices into the very fabric of digital forensic readiness. This process establishes a solid foundation for safeguarding sensitive information while ensuring the legality and ethicality of digital investigations. At its core, the PIP focuses on fortifying data security and privacy before any investigative action occurs. A breakdown of the key steps for the PIP follows next:

- Compile User Data: This initial step involves gathering relevant user data that may be subject to investigation. This data serves as the starting point for subsequent privacy-enhancing measures.
- Encrypt User Data: The collected user data is encrypted using robust cryptographic techniques. Encryption provides an extra layer of security, rendering the data unreadable to unauthorized parties. This makes the data confidential.
- Hash Encrypted Data: The encrypted data undergoes hashing, creating a fixed-size representation or 'hash value.' This value serves as a digital fingerprint for the data, ensuring its integrity.
- Sign Hash with User Private Key: To establish authenticity, the hashed data is signed using the user's private key. This cryptographic signature acts as a seal, validating the origin of the data.
- Send Signed Hash to Ledger: The signed hash value is then stored in a blockchain ledger, leveraging the blockchain's inherent tamper-resistant properties. This step ensures an immutable record of the data's existence and its associated user.

These steps collectively constitute the PIP process. This process is seamlessly integrated into the sub-process group of the Readiness process class. More specifically, it will become an integral part of the implementation process group within the readiness process class, as shown in Figure 2. This systematic integration ensures that stringent privacy standards are upheld within the broader DFR framework.

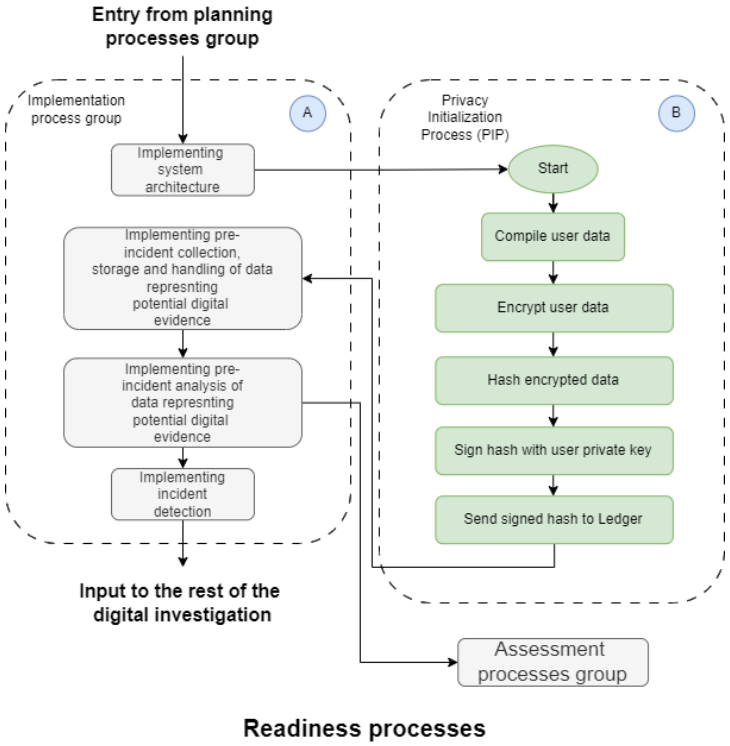


**Figure 2: Integrated PIP into Readiness Process Class**

### 3.2 Privacy Check Process (PCP)

Privacy Check Process (PCP) is an integral component of the BlockTrace model, this process plays a crucial role in ensuring that only authorized individuals have access to sensitive data, fostering a privacy-centric approach throughout the investigative journey.

The PCP is a distinctive addition to the investigative stage of the BlockTrace model. Its primary function is to validate whether an investigator possesses the necessary permission to access specific data for examination. This step ensures that data privacy and user rights are respected throughout the investigation process. Here's a breakdown of its key steps:

- **"Is the data accessible to the investigator?"**: At the outset of the process, there is an access authorization, the investigator's authorization level is verified. This involves confirming whether the investigator has the necessary permissions to access the data in question.
- **"Request access from data owner"** (expanded in next section): If the investigator's authorization is insufficient or unclear, they initiate a request for access to the data from the data owner. This request outlines the purpose and scope of the investigation. There is a multi-level access request process which is elaborated upon in the subsequent section.
- **"Retrieve data"**: Once authorization is granted, the investigator retrieves the encrypted data from storage. This encrypted data is safeguarded by privacy-enhancing technologies implemented earlier.
- **"Decrypt the data"**: The retrieved data is decrypted using the investigator's private key. This decryption step converts the encrypted data into its original, readable format.

These combined actions collectively constitute the entirety of the PCP process. This process, seamlessly interwoven into the Investigative process class, forms an integral element of the investigative journey, as depicted in Figure 3. The strategic incorporation of the PCP underscores the significance of user control over access to their distinct information.

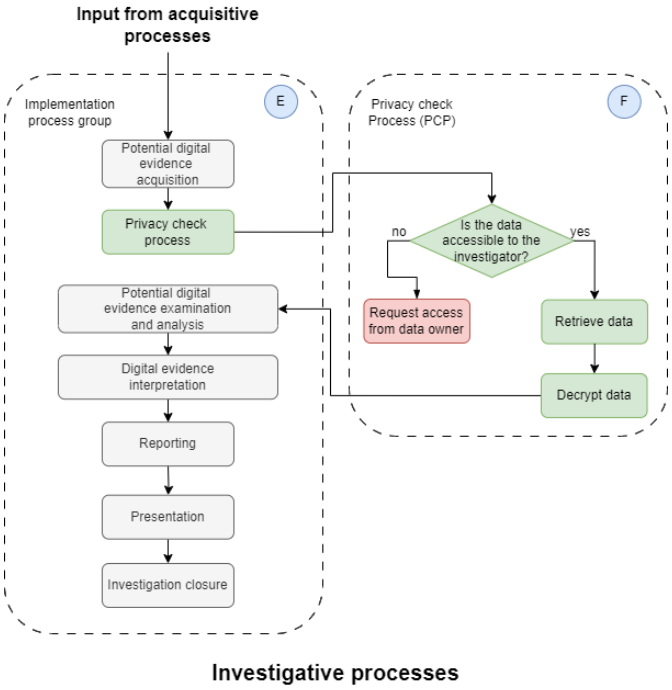


**Figure 3: Integrated PCP into Investigative Process Class**

### 3.3 Access Request Levels in Privacy Check Process (PCP)

In the Privacy Check Process (PCP), the access request phase plays a pivotal role in determining whether an investigator can proceed with data examination. This access request process is designed with multiple levels as shown in figure 4, ensuring a comprehensive approach to permissions and access control.

#### *3.3.1 Level 1: Owner's access request*

- The initial request for access to specific data is initiated by the investigator, directed to the data owner.
- The data owner holds the primary authority to grant or deny access based on their ownership rights and data stewardship responsibilities.

#### *3.3.2 Level 2: Data custodian's evaluation*

- If the data owner does not respond or provides an ambiguous response, the access request escalates to the data custodian.
- The data custodian is responsible for safeguarding and managing the data on behalf of the owner. They assess the investigator's request and may grant access if it aligns with the data's usage policies.

#### *3.3.3 Level 3: Legal department review*

- In cases where neither the data owner nor the custodian grants access, or when legal considerations are involved, the request proceeds to the organization's legal department.
- The legal department evaluates the request in accordance with legal requirements, compliance regulations, and the organization's data access policies. They may provide authorization or deny access based on these considerations.

#### *3.3.4 Level 4: Escalation and mediation*

- If access is still not granted after the legal department's review, the request enters the escalation and mediation phase.
- A designated mediation team or committee assesses the situation, seeking to reconcile any disputes or concerns among the involved parties. This phase aims to find a balanced resolution.
- Escalation and mediation serve as a final attempt to secure access while addressing privacy, legal, and organizational concerns.

- In cases where resolution remains elusive, the matter may be escalated to the jurisdictional legal system for potential civil litigation.

### *3.3.5 Access denied and investigation closure*

- If, even after reaching the escalation and mediation phase, access remains denied, the event is locked, and the investigation is officially closed.
- This stringent multi-level access request process ensures that only authorized individuals can access sensitive data, while preserving data privacy and adhering to legal and organizational requirements.
- Closure in this manner is crucial to safeguarding sensitive information, as unauthorized access could potentially expose company secrets vital to perhaps maintaining a competitive edge in the market, leading to detrimental consequences, including business failure.

Implementing multi-level access requests via PCP bolsters data security and accountability in BlockTrace. This section introduces the BlockTrace Model, revolutionizing DFR processes. It harmonizes investigative efficiency with data privacy using advanced techniques and technology.


**Figure 4: Access Request Levels in Privacy Check Process (PCP)**

## 4. Case Scenario

In this case scenario, we illustrate the practical application of the BlockTrace model in a real-world digital investigation. Our protagonist is Alice, a digital investigator, who utilizes this model to probe a security breach involving Bob, an employee at a prominent tech organization, as depicted in Figure 5.

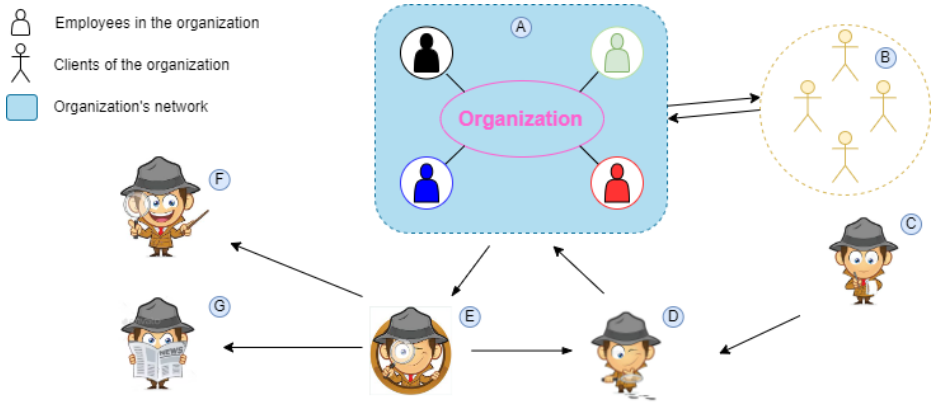


**Figure 5: Case Scenario using Alice and Bob**

As depicted in the illustration, starting from point A, the first essential step to enable a privacy-compliant investigation is the implementation of the BlockTrace model within the organization's network. The Privacy Initialization Process (PIP) ensures that all records of employees and their communications with clients, as shown in label B, are encrypted using their private keys.

Alice enters the scene at point C, where she's assigned to investigate a potentially fraudulent activity within the organization's network, indicated by point A. Her investigation leads her to Bob's computer, as portrayed in label D. To access particularly sensitive financial records, Alice initiates an access request through the Privacy Check Process (PCP), an integral component of the investigative process. In this request, she clearly outlines the investigation's purpose and scope.

This request initiates a multi-level access process, cycling through points A, D, and E. It begins with the Data Owner, Bob, who holds the initial decision-making authority. If Bob denies Alice's access request, it escalates to the Data Custodian, where it undergoes a comprehensive review to ensure alignment with the organization's established policies. If the request remains unapproved, it is subsequently escalated to the Legal Department for further scrutiny, ensuring alignment with legal and privacy requirements. Should access disputes persist, the next phase involves Escalation and Mediation, offering an opportunity to resolve access issues at a higher administrative level. As a final recourse for potential civil litigation, the Jurisdictional Legal System is prepared to intervene.

If access is granted at any point during this intricate process, the investigation can proceed, and all relevant data is decrypted. If not, the investigation is halted, and access is denied, marked by a locked event, as indicated in label G.

Upon concluding the investigation, Alice successfully uncovers substantial evidence of the alleged fraudulent activity, all the while preserving data privacy rights and adhering to strict legal standards, as depicted in label F. This scenario effectively underscores how the BlockTrace model safeguards data privacy and integrity in complex investigative endeavours, emphasizing the crucial integration of the Privacy Initialization Process (PIP) within the readiness process and the Privacy Check Process (PCP) within the investigative process.

## 5. Risks of Privacy Breach

This section highlights the concrete risks posed by privacy breaches in digital investigations. By offering specific examples, we aim to underscore the urgency of implementing robust safeguards for sensitive information.

### 5.1 Risks to Individuals

#### *5.1.1 Identity theft*

When personal information is inadequately protected during a forensic investigation, it becomes susceptible to theft. The compromised information becomes a gateway for malicious actors to assume false identities, leading to financial fraud and reputational damage.

#### *5.1.2 Blackmail and extortion*

Sensitive personal data exposed during an investigation can be used as leverage for blackmail or extortion. Individuals become vulnerable to coercion, with the potential release of sensitive information used as leverage for illicit gains.

#### *5.1.3 Psychological impact*

Individuals may suffer anxiety, stress, and loss of trust as their private lives are laid bare, impacting both personal and professional well-being. The knowledge that one's personal information has been exposed without consent can result in anxiety, loss of trust in digital systems, and a feeling of vulnerability.

### 5.2 Risks to Organizations

#### *5.2.1 Legal and financial consequences*

Privacy breaches exposes organizations to severe legal ramifications and financial penalties. Failure to protect privacy during forensic investigations may lead to hefty fines under regulations such as POPIA. The financial impact can affect organizations severely.

#### *5.2.2 Reputational damage*

A privacy breach can tarnish an organization's reputation, leading to loss of customer trust and confidence. This could lead to a long-lasting effect on customer retention and the ability to attract new business.

#### *5.2.3 Intellectual property theft*

In cases where a privacy breach exposes confidential business information, there is a risk of intellectual property theft. Competitors or malicious actors may gain access to trade secrets, proprietary processes, or innovative ideas, leading to a competitive disadvantage.

Privacy breaches pose intricate risks to organizations, spanning legal and financial implications, reputational damage, and the theft of intellectual property. Upholding privacy is not just a regulatory obligation but a strategic imperative, reinforcing resilience against these formidable threats.

## 6. Related Literature

In this section, we are bringing together insights from different types of studies from those delving into practical implementations to those probing the theoretical underpinnings. By understanding the valuable information in these pages, we equip ourselves with a comprehensive perspective, laying a foundation for the unique model we proposed. As we read through the pages of related literature, we not only acknowledge the collective wisdom of scholar preceding us but also strive to chart a path toward an integrated and privacy-conscious digital forensic future.

Frank Y.W. Law (Law *et al.*, 2011) and colleagues proposed a solution to privacy challenges in digital investigations. Their method suggests the application of encryption not only during data collection but also throughout data analysis. The core objective is to prevent digital investigators from accessing irrelevant data at any stage of the examination process.

Although this paper (Law *et al.*, 2011) focused on digital investigations in general, in the BlockTrace model, we have embraced and extended this encryption approach, integrating it to curb unauthorized access to specific data. This extension enhances data privacy and accountability in digital investigations.

Blockchain, originally conceived as the backbone of cryptocurrencies by Satoshi Nakamoto (Nakamoto, n.d.), has since matured into a multifaceted platform with far-reaching implications for data security and privacy. Its distinctive sequential and immutable structure makes blockchain exceptionally proficient at securing data and preserving its integrity.

Blockchain technology has found extensive applications across diverse domains (Mohanta *et al.*, 2019), driven by its capacity to ensure data confidentiality and integrity. Numerous research papers have explored the proposition and implementation of blockchain in various sectors. For instance, research has delved into the utilization of blockchain in the financial services industry (Treleaven *et al.*, 2017), while the IEEE has played a pivotal role in raising awareness about blockchain technology's potential in the healthcare sector (Mettler, 2016).

Within the context of the BlockTrace model, blockchain assumes a pivotal role as the linchpin of data privacy assurance. Through the seamless integration of blockchain technology, we not only bolster data security but also establish a robust underpinning for accountability within digital investigations. This amalgamation furnishes the means to curtail unauthorized access, meticulously trace data interactions, and unequivocally ensure the

immutability of digital evidence. Crucially, these advancements are achieved while upholding the fundamental privacy rights of all individuals involved.

This brief yet comprehensive review sets the stage for the proposed BlockTrace model's role in bridging the gaps identified in current literature, advancing the field of digital forensics while safeguarding individual privacy This brief yet comprehensive review sets the stage for the proposed BlockTrace model's role in bridging the gaps identified in current literature, advancing the field of digital forensics while safeguarding individual privacy.

## 7. Evaluation

The work presents several notable strengths. First and foremost, it effectively prioritizes data privacy by incorporating the Privacy Initialization Process (PIP) into the Digital Forensic Readiness (DFR) framework. This proactive approach ensures that data security is considered from the outset of an investigation. Furthermore, the integration of blockchain technology enhances data integrity within the BlockTrace model.

The blockchain's tamper-resistant nature provides a robust foundation for preserving the integrity of digital evidence. The introduction of the Privacy Check Process (PCP) adds a multi-level access control mechanism. This significantly contributes to safeguarding sensitive data and ensuring compliance with privacy regulations. The case scenario provides a practical example of how the BlockTrace model can be applied in complex digital investigations. This real-world applicability underscores the effectiveness of the model.

Lastly, the model's ability to seamlessly integrate privacy and security practices into existing DFR processes is a notable strength. It streamlines investigative procedures while respecting individual data privacy rights.

Several limitations should be acknowledged. The multi-level access control process introduced by the model can be intricate and time-consuming, potentially impacting investigation timelines.

Implementing blockchain and cryptographic techniques can be resource-intensive, necessitating investments in hardware and personnel training.

User training is essential, as users need to become proficient in navigating the model's new privacy and security features. This learning curve may pose initial challenges during adoption.

To enhance the model's effectiveness, several improvements could be considered. Streamlining the multi-level access control process could strike a better balance between security and efficiency, potentially optimizing the Privacy Check Process (PCP).

Exploring advanced privacy technologies such as homomorphic encryption and differential privacy might further enhance data privacy without compromising investigative efficiency.

The development of user-friendly interfaces for investigators could facilitate interaction with the BlockTrace model, improving its adoption and user-friendliness.

Expanding the range of case scenarios to cover a broader spectrum of investigative contexts will provide a more comprehensive understanding of the model's practicality.

## 8. Conclusion

In conclusion, the BlockTrace model, introduced in this paper, represents a significant step forward in enhancing the digital forensic readiness (DFR) processes while meticulously preserving data privacy. The model has successfully addressed the imperative need for a robust framework that harmonizes investigative efficiency with the protection of individual privacy rights. The Privacy Initialization Process (PIP) and Privacy Check Process (PCP) have been seamlessly integrated into the DFR framework, showcasing their pivotal roles in safeguarding data integrity and ensuring privacy compliance. The suggested future improvements in the evaluation aims to address these concerns and further refine the model's suitability for various investigative scenarios. One of these approaches may offer the means to access and analyse sensitive data without exposing confidential organizational secrets. By enabling a more nuanced, privacy-focused approach, we can balance the demands of thorough digital investigations with the protection of critical proprietary information, thereby contributing to a comprehensive and responsible digital forensic landscape. Overall, the work has the potential to set new standards in the field of digital forensics by bridging the gap between efficient investigations and data privacy.

## References

Anderson, R. *et al.* (2019) 'Measuring the Changing Cost of Cybercrime'.

Andre, A. (2018) 'Digital Forensics'. p. 373.
Daniel, Larry E. and Daniel, Lars E. (2011) 'Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom'. *Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom*, pp. 1–330. DOI: 10.1016/C2010-0-67122-7.
Diaz, C. and Gürses, S. (2012) 'Understanding the Landscape of Privacy Technologies 1'. p. 1.
*DIGITAL FORENSIC READINESS IN ORGANIZATIONS: ISSUES AND CHALLENGES - ProQuest*. Available at: https://www.proquest.com/docview/2034195913?pq-origsite=gscholar&fromopenview=true (Accessed: 13 October 2023).
Law, F.Y.W. *et al.* (2011) 'Protecting Digital Data Privacy in Computer Forensic Examination'. *2011 6th IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, SADFE 2011*. DOI: 10.1109/SADFE.2011.15.
Mettler, M. (2016) 'Blockchain Technology in Healthcare: The Revolution Starts Here'. *2016 IEEE 18th International Conference on E-Health Networking, Applications and Services, Healthcom 2016*. DOI: 10.1109/HEALTHCOM.2016.7749510.
Mohanta, B.K. *et al.* (2019) 'Blockchain Technology: A Survey on Applications and Security Privacy Challenges'. *Internet of Things*, 8, p. 100107. DOI: 10.1016/J.IOT.2019.100107.
Nakamoto, S. 'Bitcoin: A Peer-to-Peer Electronic Cash System'. Available at: www.bitcoin.org (Accessed: 15 October 2023).
Omeleze, S. and Venter, H.S. *Digital Forensic Application Requirements Specifications Process Word Count=8590*.
Pavlou, Paul A. (2011) 'State of the Information Privacy Literature: Where Are We Now and Where Should We Go?' *MIS Quarterly: Management Information Systems*, 35(4), pp. 977–988. DOI: 10.2307/41409969.
Pavlou, Paul A. (2011) *State of the Information Privacy Literature: Where Are We Now And Where Should We Go?*
Rowlingson, R. (2004) 'A Ten Step Process for Forensic Readiness'. *International Journal of Digital Evidence Winter*, 2(3). Available at: www.ijde.org (Accessed: 15 October 2023).
South African Government Gazette. *Protection of Personal Information. [Online]*. Available at: https://www.gov.za/sites/default/files/gcisdocument/201409/3706726-11act4of2013popi.pdf (Accessed: 15 October 2023).
Tan, J. (2001) 'Forensic Readiness'. Available at: http://project.honeynet.org (Accessed: 13 October 2023).
Treleaven, P., Brown, R.G. and Yang, D. (2017) 'Blockchain Technology in Finance'. *Computer*, 50(9), pp. 14–17. DOI: 10.1109/MC.2017.3571047.
Venter, HS. 'DFR'.
Venter, Hein. *Digital Forensic Investigations Introduction to Digital Forensics*.
Venter, H.S. *Digital Forensic Investigations The Traditional Digital Forensic Investigation Process-Part B*.
Yaacoub, J.-P.A. *et al.* (2021) 'DIGITAL FORENSICS VS. ANTI-DIGITAL FORENSICS: TECHNIQUES, LIMITATIONS AND RECOMMENDATIONS A PREPRINT'.