A Framework for Concurrent Contact-Tracing and Digital Evidence Analysis in Heterogeneous Environments

Stacey O. Baror¹, H. S. Venter¹, and Victor R. Kebande²

¹ University of Pretoria, Pretoria, South Africa
{stacey.baror,hventer}@cs.up.ac.za
² Malmö Universitet, Malmö, Sweden
victor.kebande@mau.se

Abstract. The multiple functionalities of mobile devices have allowed them to be used for contact-tracing especially with the emergence of an infectious pandemic, for example, in a smart city. This has been experienced, for example, in COVID-19 cases where propagation of infections may not be controlled effectively. Given that data is exchanged between parties it becomes important to have a focus on how this data can be used as a contact trace mechanism. This contact trace mechanism can also provide Potential Digital Evidence (PDE) that can aid to form an objective hypothesis that could be employed during litigation in the event of a suspicious infection, or when a security incident is detected. This paper, therefore, proposes an iterative Concurrent Contact-Tracing (CCT) framework based on digital evidence from mobile devices in heterogeneous environments.

Keywords: Contact-tracing · Digital forensics · Digital evidence · Heterogeneous

1 Introduction

The rapid explosion of portable devices like mobile phones, hand-held devices and the changes in wireless computing technologies has changed the dimensions of communication and changed how human beings interact. This could be attributed to mobile phone apps available and used for almost all activities, ranging from health, weather, state of the nation, news alert and updates in real-time. Furthermore, the change has led to a pervasive way of computing and has accelerated massive exchange of data across platforms. Furthermore, this has been a driving force of the increased and changing functionalities of mobile devices which has become ubiquitous [1] and have revolutionized communication.

Although mobile phones stand to be the most preferred mode of communication across the globe, ranging from home to workplace [2], the security architectures of mobile phones have not been explored extensively especially when it comes to solving sensitive problems that may be of national importance like
digital crimes or pandemics. When it comes to digital forensics, mobile phones are still regarded as a new field of study, whose architecture is still in its infancy. Generally, the information held by mobile devices carries a lot of relevant data that could be used to answer questions [3,4] during a forensic investigation or in digital forensic hypothesis formation to assist during probes or litigation.

The influence of digital forensics technology on crime management, especially with the changing trends of mobile technologies and functionalities in society, can be explored in a way that can benefit the community. Smart mobile devices (particularly data) have in the recent past been used as rapid assets for tracing persons of interests in the wake of the COVID-19 pandemic, which in most cases have proved useful, however, the degree of accuracy has not been explored. This has been possible, owing to the capabilities of most mobile phones and connectivity, like Bluetooth, GPRS, GPS, HSPA, GSM and sometimes WIFI, which has helped in the localization and handshake between mobile devices in a geographical localization of user.

Notably, with the rising proliferation and diffusion of these devices especially mobile phones [5], and smart environments under which they operate in, opportunities for criminal are increasing fast, and a number of vulnerabilities have become prevalent owing to these devices complicated architecture and functionalities. In some instances, the various functions of mobile device’s applications can also be extended to a real-time digital evidence capturing tool which could play a significant role if a suspicious security incident is detected [6].

The goal of this study therefore, is to develop a Concurrent Contact-Tracing (CCT) and digital forensic evidence framework that applies the facade of mobile devices across heterogeneous environments. The CCT framework could validate the integrity and authenticity of PDE) acquired using mobile devices when contact tracing is added as a component of evidence validation in digital forensic investigation.

The remainder of the paper is organized as follows: In Sect. 2, background and related literature is discussed. This is followed by Sect. 3 that discusses the CCT framework with a comparison of the CCT framework and existing works. A discussion is given in Sect. 4. A conclusion and an indication of the future work of the study is given in Sect. 5.

2 Background and Related Literature

2.1 Digital Forensics

Digital forensic science is drawn from the traditional science of forensics developed in conjunction with the biological sciences and has undergone a continuous growth that encompasses all digital devices [7–10]. Digital forensics has been defined as the use of “scientifically derived and proven mathematical methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and proper expertise witness presentation of digital evidence, derived from digital sources for the purpose of facilitating or furthering the
reconstruction of events found to be criminal”, or helping to anticipate unauthorised actions” [11] [7]. Generally, digital forensics provides a means to aid the preclusion of criminal related offences using digital devices. According to the national institute of standards technology (NIST) SP800-86, the number of crimes over the last decade have grown and most organisations aim to assist the law enforcement agents (LEAs) in using digital evidence that is computer generated that can decide who, what, where and how for digital crimes. The key aspects that needs to be considered are how log monitoring is conducted, how data is recovered, acquisition and collection mechanisms. Also, based on the propositions on how incidental preparations should be done, various recommendations and guidelines that target digital forensics have been mentioned by ISO/IEC 27043 [12], that has explicitly stressed the need for implementing forensic readiness as a way of reducing the cost that may be incurred during the reactive process. Studies by [13–16] however, have proposed different proactive techniques, which in the context of this study could also be mapped to how concurrent contact tracing strategies could be accomplished.

2.2 Influence of Mobile Devices

Mobile phones have evolved to be one of the most essential devices that have been adopted in almost all areas of the modern life. Additionally, Mobile devices have also impacted our way of life and are characterized by rapid, technological change and enhancements. Smart phones are among the most preferred mobile devices, because they offer the conveniences of a personal computer. An average person, operates the functions of mobile phones with no training, which is an indication on how fast mobile technology can be integrated in our society. Furthermore, businesses have adopted mobile devices as a form of communication to their clients due to the device’s ability to provide faster, easier and wider means of delivering products and services to their clients beyond the basic telephony [17]. Basically, mobile devices are available at the user’s close reach, thereby availing the user the option to demonstrate and explore the opportunities of collecting potential digital evidence and using mobile devices to curb crime in society. Exploring this option in crime management is possible due to the increased reliance on mobile devices by both business and society [18]. Guaranteeing adequate security for mobile phones has become a subject of focus, but also the prevalence of mobile phones has become advantageous for rapid investigations or extraction of contact information that can be used to solve pertinent cases, probe or find answers in critical situations like epidemics, pandemics or national security issues.

2.3 Integrity of Digital “Evidence” Data

Proliferation and technological advancements in today’s world have seen the generation of more information which is stored and distributed using various electronic means, such as mobile devices, computers and networks. This rapid growth of data has meant that there is an increase in the need for digital investigators
and LEAs to unveil a means to accommodate the demand for the necessary digital evidence required during forensic analysis. Evidence is material that enables an investigation to establish the facts relevant to a matter being investigated. In legal terms, evidence is any information or object that is admissible in a court of law which influences the outcome of the case. Eoghan, [19] defines digital evidence, as any data stored or transmitted using electronic devices that could support or refute the theory of how an offence occurred and further addresses the critical elements of the offence in terms of the intent and alibi. In another study, John [20] defines digital forensics as the use of scientifically derived and proven methods toward the validation, identification, interpretation, documentation and presentation of digital evidence derived from digital sources, such as mobile devices, computers and networks, to facilitate an investigation or for the reconstruction of events involving crime, data recovery, cybercrime, fraud, and intellectual property theft. This definition focuses on digital forensics as a method for the investigation of events involving data in digital format, and it emphasises the use of scientific methods. Furthermore, Hargreaves [21,22] identifies digital evidence as reliable objects that can uphold or refute a hypothesis in legal or civil proceedings. That means, for the admissibility of digital evidence, the integrity must be proven with a certain degree of reliability. The role of digital investigators is to provide proof that digital evidence acquired, retrieved or stored in a forensically sound manner valid for any legal preposition. The aspects prioritised when handling digital evidence are:

- The reliability of how the digital (data) evidence was generated, stored or communicated.
- The reliability of how the integrity of the digital (data) evidence is maintained.
- How the origins of digital evidence is established.
- The reliability of how the integrity of the evidence is maintained is what makes it valid evidence.

Maintaining the integrity of digital evidence is a standard technique that has been mentioned by ISO/IEC 27037 and 27043 [12] international standards. This ensures that the integrity of captured information is maintained as it should be. For example, the South African law of evidence requires that for evidence to be used, it must satisfy the court that the data is authentic, in other words, that the document is what it claims to be [21]. This is because of the volatile nature of electronic evidence which can easily be manipulated, altered or damaged after its creation and therefore authenticity must be proved [23]. However, to satisfy the court of the evidence’s originality could mean employing various scientific means.

### 2.4 Related Work

The authors have, conducted a study based on previous works that have addressed different contact tracing approaches and this has been shown in Table 1. These studies have employed various approaches and in each a number of challenges exist which we use against our framework.
### Table 1. Related work and challenges on contact tracing using mobile devices

| Ref  | Related Work                                             | Findings                                                                 | Challenges                                           |
|------|----------------------------------------------------------|--------------------------------------------------------------------------|------------------------------------------------------|
| [24] | Mobile private contact discovery at scale                | Service provider determines the user’s contact based on messaging services | Significant privacy risks, legal challenges          |
| [25] | Private discovery of common social contact               | Cryptographic primitive, allows two users on the contact list to learn common contacts | Privacy discovery of ith grade contacts-impossible without relying on a trusted third party |
| [26] | Phone call data discovery and social dynamics            | Localized discovery scheme that attempts to minimize the latency between mobile phones (Recursive binary, how devices wake up to achieve contact) | Existing neighbor discovery scheme- assumes lack of synchronization |
| [27] | Phone call data discovery and social dynamics            | Detects the dense areas based on the Maximum Spanning Tree (MST) algorithms | Study may only be generalized to study social dynamics and not urban level- Could be relevant if combined with urban sensors |
| [28] | Disease risk exposure with location data                 | A cryptographic preservation of privacy- uses recent GPS, location histories, Location based system that preserves privacy | Could be more effective if data is collected in a ubiquitous manner |
| [29] | Social technical framework for digital contact tracing    | Framework evaluates suitability of using different smart phone applications and impact on users, methods used and technology | Governments are in need of information; citizen are worried about privacy and protection of personal data |
| [30] | Contact tracing challenges-critical to halting disease transmission | Delayed and ineffective contact tracing increases the spread of an infectious disease exponentially | Complexities in reconciling the traditional means such as questionnaire and survey, especially in the dynamics of a pandemic |
| [31] | COVID-19 and contact tracing Apps: Review of EU Legal Framework | To monitor pandemic, Bluetooth, GPS and network infrastructure is preferred, others include self-report and online forms | Concerns on GDPR during personal data processing regardless of the technology used. Needful to identify actors involved in processing |

While different studies have addressed contact tracing approaches, none, has concurrently used contact tracing approaches for digital forensic purposes in parallel to the best of the authors knowledge. However, the authors acknowledge these authors contributions, for they have provided more insights on contact-tracing strategies.

### 3 Concurrent Contact-Tracing Framework for Heterogeneous Environments

A description on what the Concurrent Contact-Tracing (CCT) framework constitutes is given in this section. The CCT framework provides an approach that can use the functionalities of mobile devices to locate suspected individuals that have been exposed to risks, at the same time by depending on the time that the mobile devices spent in a close proximity to each other, the spaces they
occupied, and the content they shared with others, while the individuals are at
the same geographical location. The authors of this paper make an assumption
that the closer the proximity of the mobile device users, the higher the chances
of contracting an infectious disease, based on the propagation mechanisms like
COVID-19, for example. However, that is not the case for security incidents but
if it happens concurrently some instances would apply. This, as a result, provides
the most effective way of locating suspected cases.

3.1 CCT Framework Overview

Our proposed CCT framework utilizes interactions between different communi-
cation protocols and general mobile applications interactions like WIFI discover-
ies, GPS, historical content among different devices, Bluetooth technology based
on visited locations and the general triangulation techniques that are based on
NFC protocols. The CCT framework combines multiple functionalities (Digital
forensics, mobile devices and dimensions of a pandemic) to solve the contact-
tracing approaches as is shown in Fig. 1.

![Fig. 1. Overview of combined multiple functionalities](image)

3.2 CCT Framework Steps

Figure 2 shows the high-level CCT framework that follows six distinct steps
as follows: Discovery (1), Contact and key exchange (2), Data collection (3),
Database layer (4) Forensic layer (5) and Security and Reporting layer (6). Each
of the aforementioned steps is described further as follows:
Fig. 2. Concurrent Contact-Tracing Framework

■ **Step 1: Discovery layer** - This step allows connectivity options to be discovered ranging from GSM, GPRS, Bluetooth, HSPA, WIFI and NFC. Device discovery is a process that is used to prove that one has closely been in contact with each other based on the relationship of communication protocols.

■ **Step 2: Contact and key exchange** - Normally, Connectivity between protocols and devices would conduct key exchange to enable effective communication. Various approaches are employed to enable successful communication.
This goes further to allow the registration of MAC addresses, identification of protocols, timestamps, and IP addresses, and device IDs. Additionally, key exchange is treated as a form of data collection, where a secure channel from mobile applications are able to be created with another channel that is designated as a server [24] to allows data exchange.

■ **Step 3: Data Collection** - The collected data is as a result of secure key exchange in Step 2, which allows collected data to be collected and to be stored in a forensic database. A variety of data that is stored in the database can be used to trace contacts of suspicious infections and at the same time it can be used for purposes of forensic investigations if a suspected security incident is detected. Collected data in this context may be more application specific in order to allow timeous location and identification of users. Precisely, the distance between the two persons, A and B is vital during contact tracing.

■ **Step 4: Forensic layer** - The forensic layer is mainly dependent on the availability of collected data and suspected incident. If an incident is suspected to have occurred based on the interaction and contact between A and B, then Step 3 is activated, which proactively has incident preparation as is shown by in Fig. 1, in order to further digital forensic investigation. In the case of a suspected infection, the contacts tracing would apply. The following processes will then be applied as a result: Analysis and pre-processing of the collected contact data followed by evidence matching and correlation.

■ **Step 5: Data “evidence” protection and Reporting layer** - Based on the guidelines of ISO/IEC 27043 and 22037 which provides guidelines for identification, collection, acquisition and preservation of digital evidence, this step shows the importance of protecting digital evidence in its original form. Preferably, cryptographic hashes can be used on the extracted contact data/evidence to protect it in a fashion that ensures that its integrity is maintained. This is followed by the generation of a report that address the outcome of contact tracing or incidental investigation approaches. The generation of reports [32,33] is a crucial process that allows standardized approaches to be applied in order to uphold the requirements of admissibility.

3.3 Comparing the CCT Framework with Other Existing Frameworks

In this section, we draw diverse conclusions on the existing contact-tracing frameworks that are focused on addressing digital evidence analysis. As at the time of wring this paper, there existed no framework that combines contact-tracing techniques and digital evidence concurrently. Consequently, the CCT framework has been juxtaposed as a suitable approach that combines different functionalities while preparing for a potential pandemic across smart heterogeneous environments. Furthermore, we stress the fact that these propositions adhere to the incidental planning and preparation techniques (forensic readiness) that have been mentioned in the ISO/IEC 27043 standard where comparisons are shown in Table 2.
Table 2. Comparing the CCT and other existing frameworks

| Proposed CCT | [34] | [35] | [36] | [37] | [38] | [39] | [40] | [41] | [42] | [43] |
|---------------|------|------|------|------|------|------|------|------|------|------|
| CCT           | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    |
| Digital forensics | X   | X    | X    | X    | X    | X    | X    | X    | X    | X    |
| Data security  | ✓    | X    | X    | X    | ✓    | X    | X    | ✓    | X    | X    |
| Privacy Preservation | ✓  | ✓    | X    | ✓    | X    | X    | X    | ✓    | ✓    | X    |
| Heterogeneous | X    | X    | X    | X    | X    | X    | X    | ✓    | X    | X    |
| Concurrent    | X    | X    | X    | ✓    | X    | X    | X    | X    | X    | X    |

From the conclusions that have been drawn in Table 2, we have used the CCT framework as a baseline study to give a comparison with other relevant works [44]. Our study has been inclined in assessing the potential validity of the proposed framework given that it concurrently employs contact tracing as well as digital forensic evidence analysis in case of potential incidents. We have used X to denote the absence of a parameter and ✓ to denote the presence of a given parameter during comparison. Based on the comparison in Table 2, our assessment has been based on the following parameters: Ability to conduct contact-tracing; ability to support digital forensic capabilities, security capabilities, privacy-preserving techniques, heterogeneity and concurrency [26–35].

From the comparative assessment, it is apparent that, not all of the literature that has been used against our proposed CCT framework has incorporated all the attributes that are depicted by the CCT framework. Notably, none of the identified work has tried to address digital forensic analysis during contact tracing approaches. Basically, our findings have noted the following: [26] identified a BeepTrace that utilises blockchain and preserves the user’s privacy during contact-tracing for COVID-19, while it ensures security it is hardly focused in heterogeneous environments and concurrency. Next, [27] presents the trade-offs in utilising technology to facilitate CT with privacy-preservation. After this, [28] presents a theoretical framework for contact tracing in the wake of a pandemic, however, no concurrency, security, heterogeneity and privacy is explored. This is followed by by [29] that utilises real-word contact-tracing and concurrency, however no focus on heterogeneity, security and privacy. Notably, research by [30–33] has not addressed digital forensics and heterogeneity except [34], that addresses privacy, security and heterogeneity. Lastly, research in [35], addresses privacy in contact tracing with no concurrency, heterogeneity, security and digital forensics.

4 Discussions

The focus of this study is to mainly provide a contact-tracing framework that can concurrently combine multiple functionalities of a mobile device in order to aid in tracing potential contacts as well as conducting forensic analysis during a reactive process. The proposed CCT framework has provided clarity and its structure acts as a guide that can be used in planning and preparation for uncertainties.
A lot of digital crimes have gone unsolved due to the lack of sufficient evidence to convict the perpetrators. As a result, the use of mobile phones could be extended from their basic contact tracing functionalities into real-time digital evidence capturing devices. This is projected to increase the accessible volume of digital evidence available for forensic investigation purposes and this will further enhance the criminal justice system. The advanced functionalities of mobile devices can be extended and used for the collection, preservation and storage of potential digital forensic evidence, in accordance with evidential rules and legal standards.

We argue that the absence of a pre-incident or a post-incident mechanism if, for example, a cyber-incident is detected, may be detrimental given that mobile devices could instead be used to solve this task owing to its functionalities. The data that is collected at a location or in an environment using mobile devices while a suspected incident or infection is identified, for example in a COVID-19 situation, or a violent attack, malicious property vandalism or accident could be used to conduct a contact trace, or it could be used by a forensic investigator to validate other non-digital evidence as provided by the crime scene investigation. Additionally, the acquired digital evidence may be difficult to ascertain its authenticity, originality and correctness, hence our proposed CCT framework suggests that the extracted evidence should be subjected to cryptographic hashing as is shown in the protection layer (step 4) of Fig. 1. Nevertheless, in the case where some form of integrity and confidentiality such as cryptographic hash function, digital signature, bitstream copies, time stamp and chain of evidence is in place, the problem of the authenticity of the digital data (evidence) is averted.

From the perspective of digital forensics, digital evidence must satisfy admissibility as is highlighted by the Rules of evidence. This has been highlighted by the Daubert principles [23] on the expert witness testimonies too. For example, collecting data from A and B in some situation might be an intrusion of privacy, however in the case of a suspected pandemic like in COVID-19, one would argue that this is a matter that requires the national interest. However, if this was a case of forensic investigation in the CCT framework, this evidence would qualify based on the expert testimony. For example, [45] considers, four exclusive factors that allows evaluation of reliable evidence: authentic, accurate, complete to pass the standard of weight, as well as conform with the common law and legislative rules of evidence admissibility. Our approach that has been presented in Sect. 3 has explicitly shown the need for concurrently using contact tracing data from the relationships that exist between mobile devices as digital evidence if a suspected security incident is detected, where a forensic investigation process for mobile devices could be used, [4,46–50] for example, the harmonized processes that utilises Android mobile phones.

The CCT framework that has been suggested in this paper exemplifies a unique simultaneous approach that capitalizes on the influence of protocol inter-relationships. Furthermore, the CCT framework combines CCT and forensic investigations in the wake of a contagious infection and suspicious security incidents respectively. Additionally, the CCT is iterative which allows continuous
discovery and identification of contacts and in real-time. In order to expand the
discovery and detection, the authors have also identified network/device trian-
gulation as a device discovery technique that aids in identifying the proximity
of devices in order to help in mobile localization.

While the CCT framework takes a step in proposing a concurrent approach
that aims to address the challenge of contact tracing and digital investigation,
we note the fact that there is need for conducting further research in order to
develop a mature framework that is able to reconstruct the sequence of events
and could be standardised as a whole.

5 Conclusion and Future Work

This paper has proposed a concurrent contact tracing framework that also
utilises that tracing data as digital forensic evidence in the wake of a potential
security incident. The framework has been presented in a high-level approach
to show how localization of mobile users can turn out to be a suitable contact
tracing mechanism that could address the challenges in the wake of an infec-
tious disease like a pandemic or a matter that requires the national interests. In
this way, the resources of mobile devices could be used to extract useful data
that could concurrently be used for contact tracing and forensic investigations.
Future work aims to integrate this with sensors within a smart environment
and to develop a prototype implementation using a contact tracing API for a
real-world application.

References

1. Tassone, C., Martini, B., Choo, K.K.R., Slay, J., et al.: Mobile device forensics: a
snapshot. Trends Issues Crime Crim. Justice 460, 1 (2013)
2. Liang, T.-P., Huang, C.-W., Yeh, Y.-H., Lin, B.: Adoption of mobile technology in
business: a fit-viability model. Indu. Manag. Data Syste. (2007)
3. Quick, D., Choo, K.-K.R.: Pervasive social networking forensics: intelligence and
evidence from mobile device extracts. J. Netw. Comput. Appl. 86, 24–33 (2017)
4. Omeleze, S., Venter, H.S.: Testing the harmonised digital forensic investigation
process model-using an android mobile phone. In: 2013 Information Security for
South Africa, pp. 1–8. IEEE (2013)
5. Kebande, V.R., Ray, I.: A generic digital forensic investigation framework for Internet of Things (IoT). In: IEEE 4th International Conference on Future Internet of
Things and Cloud (FiCloud) (2016)
6. Omeleze, S., Venter, H.S.: Proof of concept of the online neighbourhood watch sys-
tem. In: International Conference on e-Infrastructure and e-Services for Developing
Countries, pp. 78–93. Springer (2015)
7. Omeleze, S., Venter, H.S.: Digital forensic application requirements specification
process. Aust. J. Forensic Sci. 51(4), 371–394 (2019)
8. Valjarevic, A., Venter, H.S.: Towards a digital forensic readiness framework for
public key infrastructure systems. In: 2011 Information Security for South Africa,
pp. 1–10. IEEE (2011)
9. Kebande, V.R., Venter, H.S.: Novel digital forensic readiness technique in the cloud environment. Aust. J. Forensic Sci. **50**(5), 552–591 (2018)
10. Kebande, V.R., Venter, H.S.: On digital forensic readiness in the cloud using a distributed agent-based solution: issues and challenges. Aust. J. Forensic Sci. **50**(2), 209–238 (2018)
11. Kent, K., Chevalier, S., Grance, T., Dang, H.: Guide to integrating forensic techniques into incident response. NIST Spec. Publ. **10**(14), 800–86 (2006)
12. ISO/IEC: 27043: 2015 international standard, information technology – security techniques – incident investigation principles and processes, vol. 1, no. 1, pp. 1–30. ISO.org (2015)
13. Kebande, V., Venter, H.: A functional architecture for cloud forensic readiness large-scale potential digital evidence analysis. In: European Conference on Cyber Warfare and Security, p. 373, Academic Conferences International Limited (2015)
14. Kebande, V.R., Venter, H.S.: Adding event reconstruction to a cloud forensic readiness model. In: 2015 Information Security for South Africa (ISSA), pp. 1–9. IEEE (2015)
15. Kebande, V.R., Venter, H.S.: A cloud forensic readiness model using a botnet as a service. In: The International Conference on Digital Security and Forensics (DigitalSec2014), pp. 23–32, The Society of Digital Information and Wireless Communication, Ostrava (2014)
16. Kebande, V.R., Karie, N.M., Omeleze, S.: A mobile forensic readiness model aimed at minimising cyber bullying. Int. J. Comput. Appl. **140**(1), 28–33 (2016)
17. Aker, J.C., Mbiti, I.M.: Mobile phones and economic development in Africa. J. Econ. Perspect. **24**(3), 207–32 (2010)
18. Enck, W., Ongtang, M., McDaniel, P.: On lightweight mobile phone application certification. In: Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 235–245 (2009)
19. Casey, E.: Digital Evidence and Computer Crime: Forensic Science, Computers, and The Internet. Academic Press (2011)
20. John, J.L.: Digital forensics and preservation. DPC Technol. Watch Rep. **12**(3), 1–53 (2012)
21. Papadopoulos, S., Snail, S.: Cyberlaw@ SA III: the law of the Internet in South Africa. Van Schaik Pretoria (2012)
22. Ikuesan, A.R., Venter, H.S.: Digital forensic readiness framework based on behavioral-biometrics for user attribution. In: 2017 IEEE Conference on Application, Information and Network Security (AINS), pp. 54–59. IEEE (2017)
23. Watney, M.: Admissibility of electronic evidence in criminal proceedings: an outline of the south African legal position. J. Inf. Law Technol. **1**, 1–10 (2009)
24. Kales, D., Rechberger, C., Schneider, T., Senker, M., Weinert, C.: Mobile private contact discovery at scale. In: 28th USENIX Security Symposium (USENIX Security 19), pp. 1447–1464 (2019)
25. De Cristofaro, E., Manulis, M., Poettering, B.: Private discovery of common social contacts. Int. J. Inf. Secur. **12**(1), 49–65 (2013)
26. Li, D., Sinha, P.: RBTP: low-power mobile discovery protocol through recursive binary time partitioning. IEEE Trans. Mob. Comput. **13**(2), 263–273 (2012)
27. Vieira, M.R., Frias-Martinez, V., Oliver, N., Frias-Martinez, E.: Characterizing dense urban areas from mobile phone-call data: discovery and social dynamics. In: 2010 IEEE Second International Conference on Social Computing, pp. 241–248. IEEE (2010)
28. Berke, A., Bakker, M., Vepakomma, P., Raskar, R., Larson, K., Pentland, A., Assessing disease exposure risk with location histories and protecting privacy: a cryptographic approach in response to a global pandemic. arXiv preprint arXiv:2003.14412 (2020)

29. Vinuesa, R., Theodorou, A., Battaglini, M., Dignum, V.: A socio-technical framework for digital contact tracing. arXiv preprint arXiv:2005.08370 (2020)

30. Greiner, A.L., Angelo, K.M., McCollum, A.M., Mirkovic, K., Arthur, R., Angulo, F.J.: Addressing contact tracing challenges-critical to halting Ebola virus disease transmission. Int. J. Infect. Dis. 41, 53–55 (2015)

31. Scantamburlo, T., Cortés, A., Dewitte, P., Van Der Eycken, D., Billa, V., Duysburgh, P., Laenens, W.: Covid-19 and contact tracing apps: a review under the European legal framework. arXiv preprint arXiv:2004.14665 (2020)

32. Karie, N.M., Kebande, V.R., Venter, H., Choo, K.-K.R.: On the importance of standardising the process of generating digital forensic reports. Forensic Sci. Int.: Rep. 1, 100008 (2019)

33. Singh, A., Ikuesan, R., Venter, H.S.: Digital forensic readiness framework for ransomware investigation. In: International Conference on Digital Forensics and Cyber Crime, pp. 91–105. Springer (2018)

34. Xu, H., Zhang, L., Onireti, O., Fang, Y., Buchanan, W.B., Imran, M.A.: Beeptrace: blockchain-enabled privacy-preserving contact tracing for covid-19 pandemic and beyond. arXiv preprint arXiv:2005.10103 (2020)

35. Redmiles, E.M.: User concerns & tradeoffs in technology-facilitated contact tracing. arXiv preprint arXiv:2004.13219 (2020)

36. Lunz, D., Batt, G., Ruess, J.: To isolate, or not to isolate: a theoretical framework for disease control via contact tracing. medRxiv (2020)

37. Cencetti, G., Santin, G., Longa, A., Pigani, E., Barrat, A., Cattuto, C., Lehmann, S., Lepri, B.: Using real-world contact networks to quantify the effectiveness of digital contact tracing and isolation strategies for covid-19 pandemic. medRxiv (2020)

38. Sun, R., Wang, W., Xue, M., Tyson, G., Camtepe, S., Ranasinghe, D.: Vetting security and privacy of global covid-19 contact tracing applications. arXiv preprint arXiv:2006.10933 (2020)

39. Li, J., Guo, X.: Covid-19 contact-tracing apps: a survey on the global deployment and challenges. arXiv preprint, arXiv:2005.03599 (2020)

40. Bianconi, G., Sun, H., Rapisardi, G., Arenas, A.: A message-passing approach to epidemic tracing and mitigation with apps. arXiv preprint arXiv:2007.05277 (2020)

41. Nielsen, B.F., Sneppen, K., Simonsen, L., Mathiesen, J.: Heterogeneity is essential for contact tracing. medRxiv (2020)

42. Yasaka, T.M., Lehrich, B.M., Sahyouni, R.: Peer-to-peer contact tracing: development of a privacy-preserving smartphone app. JMIR mHealth uHealth 8(4), e18936 (2020)

43. Collins, A.: Covid-19 contact tracing: efficacy and privacy. Technical report, EPFL (2020)

44. Kebande, V.R., Venter, H.S.: A comparative analysis of digital forensic readiness models using CFRaaS as a baseline. Wiley Interdiscip. Rev.: Forensic Sci. 1(6), e1350 (2019)

45. Watkins, H.: Daubert v. merrell daw pharmaceuticals, inc.: general acceptance rejected, Santa Clara Computer & High Tech. LJ, vol. 10, p. 259 (1994)

46. Omeleze, S., Venter, H.: A model for access management of potential digital evidence. In: International Conference on Cyber Warfare and Security, p. 491, Academic Conferences International Limited (2015)
47. Kebande, V.R., Karie, N.M., Ikuesan, R.A., Venter, H.S.: Ontology-driven perspective of CFRaaS, Wiley Interdiscip. Rev.: Forensic Sci. e1372
48. Omeleze, S., Venter, H.S.: Towards a model for acquiring digital evidence using mobile devices. In: INC, pp. 173–186, Plymouth, UK (2014)
49. Ikuesan, A.R., Venter, H.S.: Digital behavioral-fingerprint for user attribution in digital forensics: are we there yet? Digit. Invest. 30, 73–89 (2019)
50. Ernsberger, D., Ikuesan, R.A., Venter, S.H., Zugenmaier, A.: A web-based mouse dynamics visualization tool for user attribution in digital forensic readiness. In: International Conference on Digital Forensics and Cyber Crime, pp. 64–79. Springer (2017)