A survey on privacy issues in digital forensics

Aminnezhad, A and Dehghantanha, A

International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(4): 311-323
The Society of Digital Information and Wireless Communications, 2012 (ISSN: 2305-0012)

A Survey on Privacy Issues in Digital Forensics

Asou Aminnezhad
Faculty of Computer Science and Information Technology
University Putra Malaysia
Asou.aminnezhad@gmail.com

Ali Dehghantanha
Faculty of Computer Science and Information Technology
University Putra Malaysia
alid@fsktm.upm.edu.my

Mohd Taufik Abdullah
Faculty of Computer Science and Information Technology
University Putra Malaysia
mtaufik@fsktm.upm.edu.my

ABSTRACT

Privacy issues have always been a major concern in computer forensics and security and in case of any investigation whether it is pertaining to computer or not always privacy issues appear. To enable privacy's protection in the physical world we need the law that should be legislated, but in a digital world by rapidly growing of technology and using the digital devices more and more that generate a huge amount of private data it is impossible to provide fully protected space in cyber world during the transfer, store and collect data. Since its introduction to the field, forensics investigators, and developers have faced challenges in finding the balance between retrieving key evidences and infringing user privacy. This paper looks into developmental trends in computer forensics and security in various aspects in achieving such a balance. In addition, the paper analyses each scenario to determine the trend of solutions in these aspects and evaluate their effectiveness in resolving the aforementioned issues.

KEYWORDS

Privacy, Computer Forensics, Digital Forensics, Security.

1 INTRODUCTION

Computer forensics has always been a field which is growing alongside technology. As networks become more and more available and data transfer through networks getting faster, the risks involved gets higher. Malicious software, tools and methodologies are designed and implemented every day to exploit networks and data storage associated with them to extract useful private information that can be used in various crimes.

This is where computer forensics and security comes in. The field applies to scientifically collect, preserve, and recover latent evidence from crime scenes with techniques and tools.

Computer forensics is the science of identifying, analyzing, preserving, documenting and presenting evidence and information from digital and electronic devices, and it is meant to preserve the privacy of users from being exploited.

Forensic specialists have a duty to their client to pay attention about the data to be extracted that can become possibly evidence, essentially it can be digital evidence's investigation and way guiding to feasible litigation.

However, the process of extracting data evidences itself opens up avenues for forensic investigators to infringe user privacy themselves. The privacy concern that computer forensics disclose can be image, encrypted key , the user passwords and utilize knowledge that more than aim of the investigation. In order to prevent such potential abuses and protect the forensics investigators as well as users, researches and analysis has been done in various fields to provide solutions for the problem.

This paper comprises of 5 Sections and will be presented as such: Section 2 determines the limitations of the study, collects data from research publications and reviews related works in the field of privacy application in various fields and their solutions. Section 3 analyses these solutions and determine whether privacy can be preserved on both user and forensic investigator's perspective. Section 4 identifies the overlooked privacy issues by current developmental trends of privacy preservation and its potential setbacks. Section 5 concludes the paper and summarizes the overall development of technology in privacy preservation.

1.1 Limitations of the study

This paper focuses on statistical analysis based on trends from 2006. Due to the technicalities of each paper in specification of research field it is not possible to rely solely on the results to reflect the holistic picture of the real trend in privacy issues when it comes to forensics investigations. It is also difficult to fully explain the development trends of privacy issues as they are delicate in each research specimen. The research nature and scenarios used cannot be fully dependably upon as they are not necessarily applicable in another similar scenario.

The numbers of specimen provided are also too few to adequately sustain very significant research value. In this case, where most of the papers reviewed are too specific in their corresponding research field and purpose, it is difficult to generalize the specimen into statistical data with higher accuracy. We also realize that most specimens are from the Elsevier journal platform, and thus also acknowledge this as a form of limitation on availability of more related research publications in other sources.

We also credit another limitation on the lack of graphical statistical data, as most of the papers researched do not necessarily belong to statistical based research. It is not practical to add statistical assumptions into these graphical statistical data as it will possibly divert the accurate picture of the research.

1.2 Data Collection

In this research, a stringent data collection procedure is set up. Such procedure is required as the resource provided to achieve high level research results is scarce, hence every important data cannot be risked being left overlooked.

We consider 3 very important analyses: research nature analyses, keyword analyses and individual analytic platform. There is a total of 21 documents analyzed based on the aforementioned 3 approaches.

Table 1 signifies the shift of research focus when it comes to preserving privacy. It is rather evident that the current focus of forensics and security solutions are now more towards databases and networking with the rise of dependency on cloud computing technology, with 8 papers focusing on that area. More data are being stored in third party databases as compared to 5 years ago, and it became a tempting source to gain valuable private information. A shift of focus is inevitable from software and systems to database and networking under such circumstance where it is harder to gain access to information without networking access and maintain it for further exploitation. Methodologies and framework still receive adequate focus as these are the foundation of many solutions that are to be proposed in the future.

The keyword analysis signifies the focus of each specific specimen analyzed. As it is shown in Table 2, keywords used do not necessarily bear the same signature as published in these specimens, but are grouped based on their representation. For example, a computer forensics publication with digital forensics representation will be grouped together as they represent similar research nature. Keyword analysis provides a picture of techniques and theories that are being emphasized within the timeframe of this research paper.

The clear distinction on the focus of researchers to privacy and digital forensics issues marked the importance of balancing privacy and forensics. Excluding the specific related issues, general privacy and digital forensics focus achieved a total of 24 keyword matches out of 21 papers. To quantify, that would mean there are at least 3 papers that draw a comparison between both issues

in finding a balance as a major purpose of research. The other important trend is the diversity of the research. There are only 11 out of 53 representable keywords identified that bear more than 2 keyword matches. This means that more focus is given to individually specified research subjects rather a holistic picture of privacy-forensics balance.

The individual analytic platform is conducted as a final data collection. This is done by picking up a summary of each paper, and gives a brief explanation of what the paper is trying to prove and possible benefits from the publications.

Before a forensics investigator or computer security designer works on finding evidence or putting up detection systems, the first step is always to gather information and plan. The problem with Standard of Procedures (SOP) [1] of forensics investigations are that there are many instances where forensics investigators step into information that are not necessarily related to a particular crime.

Table 1. Research Nature Analaysis

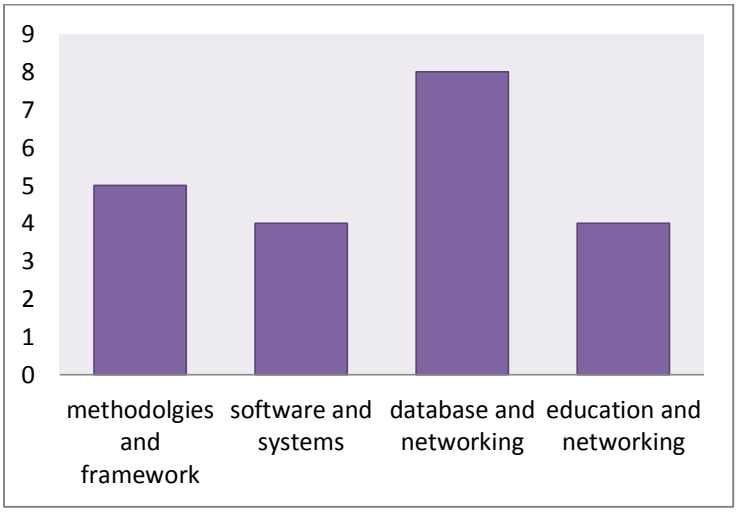
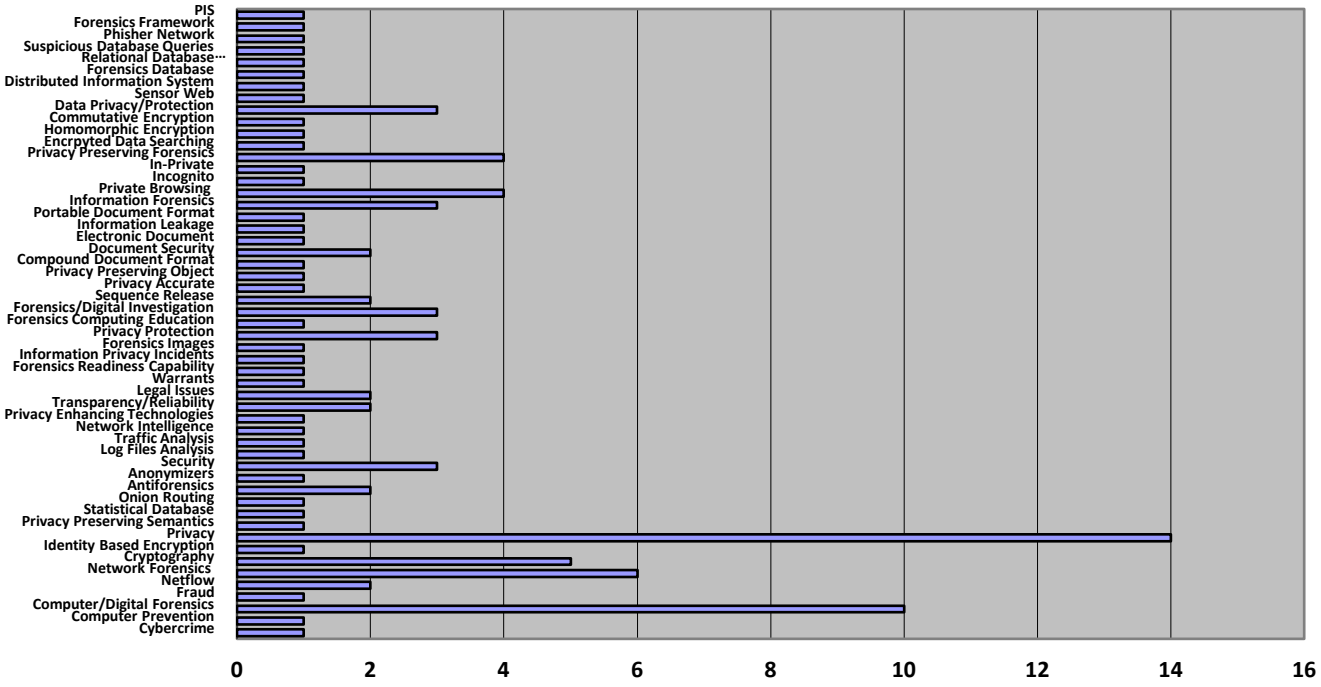


Table 2. Keyword Analaysis



The Fourth Amendment of the Constitution of United States of America is no stranger to digital forensics investigators.

2 CURRENT TRENDS OF PRIVACY IN DIGITAL FORENSICS

The Amendment protects people from unreasonable seizure and searches, and warrants that allow such seizure has to be specific to its cause. For example, if a warrant is issued against an individual to be searched for evidence of drugs, any related searches that turned out to be child pornography will not be eligible to be used against the individual. The amendment also stretches to interception of communication networks, including wiretapping [2].

However, the Amendment only limits what type of information to be searched and seized, not the protocols on how they are to be searched and seized. On this ground, [2] proposed that an audit trail on methodologies used by forensics investigators will be enough to verify if the investigation protocols exceeded court authorization.

Apart from a general audit, many related researches also produced different models for forensics investigations in recent years. In [3] proposed a framework where enterprises can meet forensics readiness to approach privacy related violations. It consisted of a series of business processes and forensics approach, executed in hierarchical order such that enterprises can conduct quality privacy-related forensics investigations on information privacy incidents.

There are 2 later models proposed in 2010. Firstly, in their research, [4] proposed a cryptographic model to be incorporated into the current digital investigation framework, where forensics investigators first have to allow the data owner to encrypt his digital data with a key and perform indexing of the image of the data storage. Investigators will then extract data from relative image sectors that matches keywords they used, with the encryption key. Image sectors without the keywords will then not be revealed to forensics investigators, guaranteeing privacy.

The next model proposed by [5] introduces a layering system on data in order to protect privacy of users from being violated and the forensics investigators themselves from infringing privacy. It allows forensics investigators to first obtain information that is layered as not related to individual before moving towards the next layer. As each layer of information is justified and obtained the layer gets deeper and closer in relation to the individual until the final layer where information is needed for forensics investigation and directly linked to the person.

In [6], PPINA (Protect Private Information Not Abuser) is proposed, an embedded framework in Privacy Enhancing Technologies (PET), a technology designed to preserve user anonymity while accessing the internet. The framework allows users to continue being anonymous unless the server has enough evidence to prove that the user is attacking the server, hence requesting a forensics investigation entity to reveal user identity. The framework is designed to achieve a balance between user privacy and digital forensics, where both goals can be achieved with a harmonious combination of network forensics and PET.

The development of digital forensics and security on software level also raises many privacy related issue. This includes information systems and related tools.

The first software that is looking into is the counter forensics privacy tool. A review was done in 2005 on this software type that prevents forensics investigators from accessing private information by wiping out data like cache, temporary files and registry values when executed. In [7], the researchers evaluated 6 tools under this category and found that while the tools potentially eliminate vast majority of targeted data, they either partially or fully failed in 6 evaluation sections which they claim to function, including incomplete wiping of unallocated space, erasing targeted user and system files, registry usage records, recoverable registry archive from system restore point, recoverable data from special file system structures and the tool's own activity records disclosure. The authors suggested that encryption might be a better alternative to replace these tools, such as Encrypting File System.

A similar analysis done on Privacy-Invasive Software (PIS) by [8], software that collects user information without user knowledge such as spyware and advertisement software known as adware, also found that current tools designed to combat them (anti-spyware and adware) failed to identify them fast enough or even identifying them at all and have problems classifying PIS properly. The research concluded that these tools, that be run on similar algorithm dealing with viruses and malware (signature identification) does not work well on PIS due to its nature of existence in grey area between business facilitating and malicious. Manual forensics method, upon experiments, provided better results instead.

Browsers also raise privacy related issues, as they are used to perform many activities such as trading online, which requires a private information transfer. In [9] published an analysis on three widely used browsers in terms of their private browsing effectiveness. Private browsing is a feature that prevents browsing history to be stored in the computer's data storage. The authors concluded that while all three browsers do not display visible evidences in private browsing mode, related data can still be extracted with proper forensics tool and methodology. From the user's viewpoint, the authors also concluded that Google Chrome and Mozilla Firefox are better private browsing solutions compared to Internet Explorer.

Portable Document Format (PDF) is invented by Adobe, credited with its security compared to other document format. In [10], the researchers released their review in this format, suggesting that PDF is subject to leak information due to its several interactive features, including flagging content as "deleted" instead of really deleting them, allow tracing of IP address on its distribution, and very subject to hackers to collect this information while using PDF to conduct malicious cyber-attacks. The authors proved the investigation with several tools and attacks, suggested a few solutions on an administrator level dealing with PDFs, such as the shocking nature of PDF files received and systems like EES (Elsevier Editorial System) to monitor PDF files.

In [11], on the concept of Onion Routing, pointing out the evolution of the concept in preserving privacy raised issues of difficulties during investigations. Onion Routing is created to absolutely prevent traffic analysis from third parties by encrypting socket connections and act as a proxy instead. Only the adjacent kin routers along the anonymous connection can "unpeel" the encryption as the packets approach its destination, preventing hijacks and man-in-the-middle phenomena. However, the author argued that the same technology could be used by criminals to prevent traffic analysis of forensics investigators and bypass censorship, or combining the concept to perform other malicious attacks on networks. Such concept makes it very difficult for forensics investigators to collect evidence as there are too few avenues to access the information pockets from third parties, unless access is gained from the inside chain of the connection or tracing the last router's communication with the destination which is the weakest protection in the chain.

In [12], the researcher published their findings on preserving privacy in forensics DNA databases. Such databases are designed to be centralized, usable by forensics investigators globally to identify criminal identities based on DNA matches. To solve issues where such information may be leaked into parties for non-investigative purposes on forensics ground, the authors proposed a framework in reworking the database access controls to only accept certain queries that are legitimate forensics queries. These queries include blood samples and cell tissues that are found at crime scenes.

In [13], the researcher outlined his research on privacy issues raised by sensor webs and distributed information systems, an active field after the 911 incident. Distributed information systems are information collecting systems with huge data repository, including private information such as financial and communications records. Sensor webs use small, independent sensors to collect and share information about their environment without wire. The author proposed several policies to maintain privacy in distributed information systems and sensor webs,

including fundamental security primitives such as low level encryption and authentication, human interfaces to limit queries, selective revelation of data, strong audits and better querying technologies, with policy experimenting, security and legal analysis, masking strategies to obtain results.

Another networking issue arises in shared and remote servers, servers that stores data for users as a form of third party data storage. Essentially there are two problems here; firstly, these servers are owned by third party service providers, hence getting access without their knowledge of what investigators are looking for is difficult due to permission grants (privacy preservation). Secondly, the servers' nature to be remote also makes it difficult to trace evidence in a large number of shared and distributed storage using traditional forensics method of imaging (cloning) the storage devices. The usual privacy issue of tampering into irrelevant data also exists. To solve these problems, [14] proposed two schemes, the homomorphic and commutative encryption. The homomorphic encryption is a scheme where both administrator of remote servers and investigators encrypt their data and queries. The administrator then uses the encrypted queries with the investigator's key to search the server for relevant data, and the investigator then decrypts the data with the administrator's key. The commutative encryption introduces a Trusted Third Party (TTP) that supervises the administrator to prevent unfair play. The details are similar to homomorphic encryption, with another layer of commutative-law based encryption applied by TTP before the searching on data storage is conducted. Both schemes allow investigators to obtain information that they need without exposing them to administrators of the remote servers.

In [15], the researchers presented an approach to detect accessing parties of leaked information from a relational database through queries. In this approach, the authors argued that suspicious queries can be determined if and only if the disclosed secret information could be inferred from its answers. To do this, a series of optimization steps involving the concept of replaceable tuples and certificates, and database instances are explained in relational mathematics. An algorithm is constructed then from these optimization steps to determine whether a query is suspicious with respect to a secret and a database instance.

In [16], a framework in 2011 to preserve privacy while handling network flow records is proposed. Network flow recording collects information about network traffic sessions. This information can contain very private data, including network user information; their activities on network, amount of data transferred and used services. The authors proposed a framework of integrated tools and concepts to prevent such data from falling into the wrong hands. The framework is divided into 3 sections: data collection and traffic flow recording, combined encryption with Identity Based Encryption and Advanced Encryption System, and statistical database modelling and inference controls. The framework is implemented to prevent privacy on two phases, including encryption and decryption of data collected and the manner of constructing statistical reports such that inference controls are applied to prevent a response to suspicious queries.

To combat phishing that often leads to identity theft, [17] proposed a framework in 2008 (citation 2008 a forensic). The framework is to counter-phish phishers, using a fake service (phoneypot) with traceable credential data (phoneytokens). When a phisher is identified, he/she is directed to the phoneypot and transact with it, transferring phoneytokens into the phisher's collection server. This allows investigators to trace and profile the identity of the phisher through these tokens. The authors argued that even if the counter-phishing attempt is discovered, it would have caused enough problems to the phisher to avoid the target in the future, protecting the user from further exploitation by phishing attacks.

In general, database systems are supposedly designed to store and handle data in a proper manner. In [18], the researchers' findings in 2007 that proved this wrong are published. They concluded that database systems do not necessarily remove stored data securely after deletion whereby remnant data and operations can be found in

allocated storage. Database systems also made redundant copies of data items that can be found in file systems. These data present a strong threat to privacy as not only investigators may find themselves dealing with unwarranted data, criminals may also access them for malicious purposes. To avoid this, the authors designed a set of transparency principles to ensure secure deletion of data, modified database language (MySQL) internals to encrypt the expunction log with minimal performance impact that usually occur when it comes to overwriting-encryption.

In 2008, [19] published a paper explaining the importance of computer forensics to be practiced in today's networked organizations. It outlined the key questions including the definition of computer forensics, its importance, legal aspects involved and online resources available for organizations to understand computer forensics in a nutshell.

In [20], a paper is published that addressed a rising problem of professionalism when it comes to digital forensics in other fields. The author pointed out that in many scenarios when it comes to InfoSec professionals being deployed to work on digital crime investigations their duties are very limited to laws and legal systems, and lack the intersection of business requirements from enterprises and government. He argued that coordination between different departments is essential to achieve investigation goals, hence proposed a GRC-InfoSec compliance effort. A few suggestions put forth include a legal research database to create a cross-referencing table of regulatory actions and legal case citations to IT-specific laws and guidelines, and presentation of resulting costs and business disruption. (GRC stands for Governance, Risk management and amp; Compliance)

As for education, [21] published a system that produces file system images for forensic computing training courses. The system known as forensig, developed with Python and Qemu, allows instructors to set constraints on certain user behavior such as deleting and copying files, in a script which is then executed in a form of image that can be analyzed by the students. The results can then be matched with the input script. It solves the issues of instructors using second hand hard disks for analysis practice, which often times contain private data.

Besides that, [22] tackle cybercrime-related issues. Issues regarding privacy as a fundamental right, comparison of legal issues between countries discuss in the workshop. In addition there were few works on privacy issues that may arise during malware analysis [23,24], analysis of cloud and virtualized environments [25-27], and in pervasive and ubiquitous systems [28-32]. With growing usage of mobile devices and Voice over IP (VoIP) protocol several researchers tried to provide privacy sound models for investigation in these environments [33-36]. Finally, there were models for forensics log protection while considering user privacy in log access occasions [37,38].

3 DISCUSSION AND ANALYSIS OF RESULTS

We believe that the development of solutions and frameworks to contain privacy issues in various fields are not synchronized. Our analysis is done based on each field, with comparison to related fields and their effects as a whole towards privacy preservation. We found out that while research in one field contributed compelling solutions that might be a long term answer to privacy preservation, it does not necessarily be the case on another field. To analyze the development of each field, we split the stakeholders in each section, from users' and forensics investigators' perspectives.

3.1 Privacy Preservation from User's Perspective

We found that in the case of a user, the major problem of preserving privacy is the lack of knowledge and understanding. General users do not know the technicalities of how networks and data storage are being managed, and their rights in their personal and private information being used by organizations. Hence, researches and development of a framework and systems with privacy preservation of user's data are focused more

towards passive preservation, without them knowing how the framework and system preserve their data.

We found this to be very effective, yet deceiving at the same time. In instances where frameworks are applied to networks and databases, for example the inference controls and encryption framework that are implemented on network flow recording and traffic analysis, onion routing, cryptographic approach on DNA forensic databases, homomorphic and commutative encryption, and sensor webs protection framework, the solutions provided are usually effective in tackling situational crisis on data privacy, and users usually do not know such solutions are implemented to protect their data from being exploited. However, the review on counter-forensics privacy tools and analysis of how database systems delete data, plus the problems in Portable Document Format when they "delete" data, proved the deceiving pictures of these tools and systems being able to live up to expectations, or placed a false dichotomy that they deliver in their tasks. Especially when users generally do not know if these tools work exactly like what they expect, and assumed that they do work, private data are constantly under threat of being exploited by malicious parties with no warning posed to the users to be aware of the situation of their private data.

We also found that privacy preservation can never be achieved at its fullest. The proposed frameworks and models, with encryption and technologies implemented, their findings have a similar issue; it is particularly hard to design a fully protected system, with constraints and assumptions primarily added into the calculus to prove their frameworks and models can function under these constraints. The mention of "future works" or manual audits have been used in particularly general models, including sensor webs and distributed information systems, database systems, relational database query controls and counter-Phishing. This presents another issue; not all users are aware of what type of scenario their data would most likely be exploited, or in which type of scenario their current data storage is in. This contributes generally to another problem; when user privacy is breached, the need for different professionalism to handle the investigations become difficult due to the lacking of standardization and understanding of the scenarios and the status quo.

Throughout these flaws, we understand that while development and researches to preserve user privacy better are getting better on the road, the idea of a fully protected framework or model will not suffice in the near future. It is important for users to understand the need for them to secure their private information at the best of their interest, particularly when cloud computing technology is on the rise, and more remote and shared data storages are made available for users. Users must know their responsibility in their own personal information, and utilize as much as possible combinations of several developed privacy preserving solutions to protect their data well while networking. From picking the right browser to perform private browsing to using the services of trusted organizations with proven functioning privacy preservation policies and technologies in place are a few sets of decisions and combination of models and framework to secure private data better.

We also think that users must always have the awareness and understanding that their private data might be leaked. Such awareness is needed with status quo proving that privacy preservation is still in its developmental stages in redefining their borders and to what extent they should provide protection. Users must always be prepared to face scenarios and seek solutions when such leaks happen, and know how forensics investigators perform investigation without further threatening their privacy in this regard.

To conclude this subsection, we believe that users need to have a general understanding and knowledge on how technologies aid in privacy preservation while they are storing data on networks, using tools and services, and if these technologies are delivering their functions. We also believe that users must understand that technologies can only help in privacy preservation that much and it is a collective effort of a combination of technologies with professionalism and expertise of other aspects to better privacy

preservation. It is also important that users are prepared to deal with situations when their privacy has been breached, and seek the best solutions available, including forensics investigations. It is also evident to us that development of privacy preservation techniques and tools are predicated more towards technical solutions rather than a holistic approach, desynchronizing the focus to tackle the problem.

3.2 Privacy Preservation from Forensics Investigators' Perspective

The jobs of forensics investigators are to collect, preserve and analyze information, then reconstruct the events of a crime. We found that when it comes to privacy preservation from the forensics investigators' perspective, it is always a dilemma strongly linked with user privacy and legal systems, as pointed out by many related works.

We concur that forensics investigators' procedural methodologies in collecting, preserving and analyze information possess potential avenues of user privacy infringement. Our agreement on this course is based on a general assumption that forensic investigators have vested interest in this information; either they are important in proving a court case or a crime, or they are important for personal use, which often times contain malicious purposes.

We found that the related research and proposed solutions provided positive and negative effects in forensics investigations. We argue that the limitations and constraints implemented in these systems and models do help in protecting forensics investigators from infringing privacy, but on the other hand, limit them from conducting forensics investigation in a more direct and effective approach.

We want to explain this on both levels. On the positive note, constraints applied on various frameworks, such as homomorphic and commutative encryption, onion routing, inference controls, DNA blood and tissue samples from the crime scene as key queries, sequential data release based on relational levels and network flow recording framework all demonstrated a vast implementation of constraints to protect unrelated data from being exposed to forensics investigators while conducting investigations. We believe that sequential data release based on relational levels is particularly critical in addressing privacy issues and balancing user privacy and legal need to access such private data, as it allows direct avenue to gain access to private information through a specific process, not as general as organized queries and encryption. We believe that integration of these technologies can bring more positive contribution in aiding forensics investigators. Using the

Sequential release of information based on a relational level as a framework to implement and shape organized queries is an example of integration of both techniques while conducting forensics investigations.

However, there are negative sides of it as well. The issues here are on the non-technical part of dealing with privacy. We found that the most obvious impact of the proposed frameworks, such as cross referencing encrypted queries with data, onion routing and strong audit are among the frameworks that directly limit avenues that can be taken by forensics investigators to approach their investigations. We need to consider the assumption that all crime investigations are time sensitive and such constraints placed by these frameworks may prolong the already time consuming investigation progress, as investigators now have to plan their investigation methods to be more technical and direct in order to extract the right evidence. Besides that, the possibility of extracting wrong or irrelevant evidence still exists regardless of how these frameworks are in place. The fact that tracing private information without really knowing the content and only based on keywords does not necessarily reflect the nature of data collected, meaning the data might not be useful to the investigation, and risks the possibility of exposing private information as well.

Finally, we found that ambiguity always exists in privacy issues when it comes to forensics investigators. We argue that a forensics investigator is an individual that is equipped with decent knowledge of computer security. We believe that if an individual's purpose of obtaining private

information is malicious, the data will still be leaked into the wrong hands anyway. The idea is regardless of how far technology has gone into preserving privacy, it still runs the possibility of being leaked and exposed, considering of their possible use and management by another person other than the user him/herself. While having such technologies deter forensics investigators to use the extracted information properly, it is still not a guarantee that the information will not be misused in the hands of forensics investigators, whether intentional or unintentional.

To conclude, we believe that the proposed frameworks, introduced technologies and implemented models and tools believed to be able to aid forensics investigators from infringing user privacy while conducting investigations might not be as one sided as it seems. We believe that the rationale and professionalism of the forensic investigators are important when handling private data as their expertise in handling computer security is on level enough to know how these technologies work in protecting private data. We also believe that such technologies still need to remain to deter forensics investigators from drifting off their professionalism, but essentially the negative impacts of such deterrence in place might jeopardize privacy even further with the possibility of irrelevant information leaking out anyway, and prolonging the forensics investigation process. We conclude that it is important that the forensics investigators know the sensitivity of data they are going to handle in each investigation and understand their professionalism is important in preserving privacy.

3.3 Privacy Preservation from Technologies' Perspective

We found that from a technology perspective, the current development of cyber security and digital forensics in preserving privacy may have reached a bottleneck, and the latest developments are too constrained to very few general security measures. This in turn does not bring too much positive improvement in the field, but returns negative effects as well.

We analyzed some of the reviews and would like to highlight several examples to support our findings. The first problem with current technologies is the similarity of techniques. We found that almost all security measures taken in various frameworks and models, be it database systems, remote servers, relational databases or network flow recording, the framework looks similar in terms of their algorithm, which includes encryption, data deletion and controls. We concur that some of the combinations are effective, such as onion routing and sequential data release in preserving privacy from being exposed to unrelated parties. However, assuming in general scenarios, similarity in security frameworks often means faster workarounds being developed by malicious hackers, as these frameworks share a common structure, and provide more examples for malicious parties to work their ways around the security system. We also noticed that in some of the frameworks proposed, the authors made assumptions that otherwise will jeopardize the system, and offer a contingency solution. However, in one such scenario such as onion routing, the author mentioned about how it would also harm investigators should the framework be used against them. As onion routing renders traffic analysis from third parties impossible, it would be extremely difficult to trace or extract information from such routing method used by malicious users for tracking and profiling purposes. This is a typical example of how technologies, even in the cyber security field, can reserve wanted results and have an unexpected and undesired effect when it is being used by the wrong party.

The same happens to the commutative encryption example. The framework could only work properly under the assumption that the administrator provides all database information in an encrypted manner. Should this is not the case, not only the extracted information by the forensics investigators suffer possibilities of being irrelevant, it also jeopardizes the process of investigation as the forensics investigators would likely miss out important evidence in reconstructing the sequence of events on the crime.

To conclude, development of technologies in cyber security and digital forensics are very much predicated on technicalities only, and does not necessarily provide more improvement to preserving privacy as it has been expected to. The similarity in frameworks and models proposed, plus the possibility of technologies being used in the wrong hands are all issues that have to be solved at grassroots level to ensure privacy preservation is successful. We believe that apart from technical development, technologies will need to take into consideration other aspects that influence digital forensics and cyber security, including education, business requirements, professionalism from other related fields and work together to ensure a more holistic level of improvement in preserving privacy can be achieved. We also argue that technologies in digital forensics and security can backfire and become dangerous if it is reversely used by malicious users with intent to harm and infringe user privacy.

4 CRITICALLY OVERLOOKED ISSUES

As mentioned in the analysis section, we believe that privacy issues stem from intention, and made possible with the use of technology. However, technology has already revolutionized to a level that it is applicable to almost every industry; a good example is how database technology is used in storing DNA samples of criminals, which can stem into medical forensics for a start. Research focus should now be more emphasized on solving the issue at a root problem rather than introducing more technical countermeasures in the field, which many publications in this research also proved to be applicable on both privacy preservation and exploitation use.

We also note that the focus on education and awareness of intention of protecting privacy and preservation in a professional forensics field are not adequate enough to strike the balance between privacy preservation and getting the investigation done in quality level. We find that this is particularly detrimental, as technologies that are continuously being rolled out into the commercial market will not be able to be utilized in satisfactory level by professional forensics investigators without proper training and awareness. This opens up to more possibilities of abuse without consent or abuse without a motive by investigators. Awareness is also not given emphasis on the user's side, and this exposes users to higher risk of being abused under the same paradigm. Simply put, even with the latest technologies and framework in place to preserve privacy, it would have been rendered useless should both parties that use them are not aware of their potential, and subject to risk of being abused by such technologies instead.

5 CONCLUSION

This paper has identified various privacy issues in cyber security and digital forensics, issues that use for protecting privacy of data in forensic investigation, whereby how forensics investigators may have infringed user privacy while conducting forensics investigations, and how user privacy is always under threat without proper protection. It has also reviewed the current development trend shift in this industry, why such trend could have happened and its drive.

The paper has reviewed various fields and their development in the technicalities and technologies to address this problem. The paper describing each field in a nutshell that explains how these technologies work, and what are their approaches in solving the problem of preserving privacy. The reviews are split into three sections, each with its corresponding fields of reviews and explanation.

The paper then analyses these reviews and view them from the user and forensics investigator's perspectives, whether such development in cyber security and digital forensics actually improve the efforts on preserving privacy. The paper concluded that while every development has its positive approach and finds the solution to what the authors want to solve, the issue of privacy preservation still exists, with the consideration of non-technical aspects in professionalism in practice and the ambiguity of scenarios causing some approaches to be counterproductive. The paper also analyses on how at a technical level, advanced technologies in

digital forensics and security are facing a bottleneck in development and could bring about as equal harms to the current efforts in preserving privacy.

6 REFERENCES

[1] I-Long Lin, Yun-Sheng Yen, Annie Chang: "*A Study on Digital Forensics Standard Operation Procedure for Wireless Cybercrime*," International Journal of Computer Engineering Science (IJCES), Volume 2 Issue 3, 2012.

[2] C. W. Adams, "*Legal issues pertaining to the development of digital forensic tools*," Third International Workshop on Systematic Approaches to Digital Forensic Engineering, pp. 123-132, 2008.

[3] K. Reddy and H. Venter, "*A Forensic Framework for Handling Information Privacy Incidents*," Advances in Digital Forensics, volume V, pp. 143-155, 2009.

[4] Frank Y.W. Law et al, "*Protecting Digital Data Privacy in Computer Forensic Examination*," Systematic Approaches to Digital Forensic Engineering (SADFE), 2011.

[5] N. J. Croft, M.S. Olivier, *"Sequenced release of privacy-accurate information in a forensic investigation,"* Digital Investigation, volume 7, pp. 1-7, 2010.

[6] G. Antoniou, C. Wilson, and D. Geneiatakis, PPINA – "*A Forensic Investigation Protocol for Privacy Enhancing Technologies*," *Proceedings of the 10th IFIP on Communication and Multimedia Security*, pp. 185-195, 2006.

[7] M. Geiger and L. F. Cranor, *"Counter-forensic privacy tools*," Privacy in the Electronic Society, 2005.

[8] M. Boldt and B. Carlsson, *"Analysing countermeasures against privacy-invasive software,"* in ICSEA, 2006.

[9] H. Said, N. Al Mutawa, I. Al Awadhi and M. Guimaraes, "*Forensic analysis of private browsing artifacts*," in International Conference on Innovations in Information Technology, 2011.

[10] A. Castiglionea, A. D. Santisa and C. Sorien, "*Security and privacy issues in the Portable Document Format*," The Journal of Systems and Software, volume 83, pp. 1813–1822, 2010.

[11] D. Forte, "*Advances in Onion Routing: Description and backtracing/investigation problems*," Digital Investigation, volume 3, pp. 85-88, 2006.

[12] P. Bohannon, M. Jakobsson and S. Srikwan, "*Cryptographic Approaches to Privacy in Forensic DNA Databases*," Lecture Notes in Computer Science Volume 1751, pp 373-390, 2000.

[13] J.D. Tygar, "*Privacy in sensor webs and distributed information systems*," Software Security, pp. 84-95, 2003.

[14] Y. M. Lai, Xueling Zheng, K. P. Chow, Lucas Chi Kwong Hui, Siu-Ming Yiu, *"Privacy preserving confidential forensic investigation for shared or remote servers,"* in International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp.378-383, 2011.

[15] S. Böttcher, R. Hartel and M. Kirschner, "*Detecting suspicious relational database queries*," in The Third International Conference on Availability, Reliability and Security, 2008.

[16] B. Shebaro and J. R. Crandall, "*Privacy-preserving network flow recording*," Digital Investigation, volume 8, pp. 90-100, 2011.

[17] S. Gajek, and A. Sadeghi, "*A forensic framework for tracing phishers*," volume 6102 of LNCS, pages 19-33. Springer, 2008.

[18] P. Stahlberg, G. Miklau, and B. N. Levine, *"Threats to privacy in the forensic analysis of database systems*," ACM Intl Conf. on Management of Data (SIGMOD/PODS), 2007.

[19] US-CERT, Computer Forensics, 2008.

[20] S. M. Giordano, "*Applying Information Security and Privacy Principles to Governance*," Risk Management & Compliance, 2010.

[21] C. Moch and F. C. Freiling, "*The forensic image generator generator*," in Fifth International Conference on IT Security Incident Management and IT Forensics, 2009.

[22] J. R . Agustina and F. Insa, *"Challenges before crime in a digital era: Outsmarting cybercrime offenders," Workshop on Cybercrime, Computer Crime Prevention and the Surveillance Society*, volume 27, pp.211-212, 2011.

[23] F. Daryabar, A. Dehghantanha, HG. Broujerdi, *Investigation of Malware Defence and Detection Techniques,"* International Journal of Digital Information and Wireless Communications(IJDIWC), volume 1, issue 3, pp. 645-650, 2012.

[24] F. Daryabar, A. Dehghantanha, NI. Udzir, "*Investigation of bypassing malware defences and malware detections*," Conference on Information Assurance and Security (IAS), pp. 173-178, 2011.

[25] M. Damshenas, A. Dehghantanha, R. Mahmoud, S. Bin Shamsuddin, "*Forensics investigation challenges in cloud computing environments*," Cyber Warfare and Digital Forensics (CyberSec), pp. 190-194, 2012.

[26] F. Daryabar, A. Dehghantanha, F. Norouzi, F Mahmoodi, "*Analysis of virtual honeynet and VLAN-based virtual networks*," Science & Engineering Research (SHUSER), pp.73-70, 2011.

[27] S. H. Mohtasebi, A. Dehghantanha, "*Defusing the Hazards of Social Network Services*," International Journal of Digital Information, pp. 504-515, 2012.

[28] A. Dehghantanha, R. Mahmod, N. I Udzir, Z.A. Zulkarnain, "*User-centered Privacy and Trust Model in Cloud Computing Systems*," Computer And Network Technology, pp. 326-332, 2009.

[29] A. Dehghantanha, "*Xml-Based Privacy Model in Pervasive Computing*," Master thesis- University Putra Malaysia 2008.

[30] C. Sagaran, A. Dehghantanha, R Ramli, "*A User-Centered Context-sensitive Privacy Model in Pervasive*

Systems," Communication Software and Networks, pp. 78-82, 2010.

[31] A. Dehghantanha, N. Udzir, R. Mahmod, *"Evaluating user-centered privacy model (UPM) in pervasive computing systems*," Computational Intelligence in Security for Information Systems, pp. 272-284, 2011.

[32] A. Dehghantanha, R. Mahmod, "*UPM: User-Centered Privacy Model in Pervasive Computing Systems*," Future Computer and Communication, pp. 65-70, 2009.

[33] S. Parvez, A. Dehghantanha, HG. Broujerdi, "*Framework of digital forensics for the Samsung Star Series phone*," Electronics Computer Technology (ICECT), Volume 2, pp. 264-267, 2011.

[34] S. H. Mohtasebi, A. Dehghantanha, H. G. Broujerdi, "*Smartphone Forensics: A Case Study with Nokia E5-00 Mobile Phone*," International Journal of Digital Information and Wireless Communications (IJDIWC),volume 1, issue 3, pp. 651-655, 2012.

[35] FN. Dezfouli, A. Dehghantanha, R. Mahmoud ,"*Volatile memory acquisition using backup for forensic investigation*," Cyber Warfare and Digital Foresnsic, pp. 186-189, 2012

[36] M. Ibrahim, MT. Abdullah, A. Dehghantanha , "*VoIP evidence model: A new forensic method for investigating VoIP malicious attacks*," Cyber Security, Cyber Warfare and Digital Forensic , pp. 201-206, 2012.

[37] Y. TzeTzuen, A. Dehghantanha, A. Seddon, "*Greening Digital Forensics: Opportunities and Challenges*," Signal Processing and Information Technology, pp. 114-119, 2012.

[38] N. Borhan, R. Mahmod, A. Dehghantanha, *"A Framework of TPM, SVM and Boot Control for Securing Forensic Logs*," International Journal of Computer Application, volume 50, Issue 13, pp. 65-70, 2009.