INTERNATIONAL JOURNAL OF eBUSINESS AND eGOVERNMENT STUDIES
Vol 9, No 1, 2017 ISSN: 2146-0744 (Online)

OPEN ETHICAL ISSUES IN DIGITAL FORENSIC SYSTEMS

Adedayo M. Balogun
Vaal University of Technology, South Africa
dayhorz@yandex.com

Tranos Zuva
Vaal University of Technology, South Africa
tranosz@vut.ac.za

—Abstract —

Digital forensic systems collect, filter, process, store and distribute data, to facilitate the investigational-cum-organizational decision-making process, as expected of any typical information system. These specialized systems are used to establish and understand the specifics of electronic incidents, after which information gathered could then be used to accurately identify and reprimand the parties abusing such electronic infrastructures as well as to stop any similar future incidents. However, due to the relative infancy of the digital forensic discipline as a whole and a number of other contributory factors, these systems infringe on and defy a lot of norms that have become acceptable to both individuals and organizations. This paper seeks to highlight the open issues within the digital forensic systems development and implementation area that border on ethics. The study employed a method which collected secondary data from related publications and analysed them to identify valid recurrent points. Recommendations are subsequently provided to each of the issues identified, with the aim of keeping the discipline's stability and stakeholders' expectations balanced.

Key Words: Issues, Ethics, Information systems, Digital forensics, Decision making, Societal norms.

JEL Classification: O33 Technological Change: Choices and Consequences • Diffusion Processes.

1. INTRODUCTION

Lynch (1994) regarded new technologies as the institutors of new ethical dilemmas. She further stated that computer technologies, in particular, are notorious for forcing changes to the pre-computing behaviours that people were accustomed to. This was corroborated when Mohay, Anderson, Collie, Vel & Mckemmish (2003) acknowledged that the pervasive adoption of the computer and web technologies would be a causality for unprecedented issues in the modern society. Although cybercrimes were the issues focused on in their study, it could be argued that cybercrimes result from the majority of perpetrators being ethically flawed (Turvey, 2009). Ethics provide distinctions between the rights and wrongs of various scenarios in specified domains, as well as principles of making choices with respect to their impact on preserving the esteem of a particular group and/or the larger world (Miller, 2009). Its main purpose is to ascertain the best ways for individuals and groups to act and resolve issues in order to foster an orderly system of life by distinguishing rights from wrongs, virtues from vices, good from bad, and equity from unfairness (Baqgini & Fosl, 2007).

Information systems are increasingly overtaking the traditional information use strategies in organizations, as the notable success of computer technologies continuously induces the automation of older and less efficient methods. Their widespread implementation in social, political, economic, educational, and medical spheres affects the nature of individuals and groups in direct and indirect ways, thereby creating new realities (Sheetz, 2007). Thus, the consideration of ethics in the use of information systems is important since it can be critical to the relative success of communities. However, the scope of digital forensic systems extend more than that of typical information systems, thus making them more susceptible to more serious ethical concerns.

The rest of this paper is organized thus: Section II highlights the general ethical concerns about information systems from literature. Section III discusses the notable distinctions between typical information systems and digital forensic systems. In section IV, the concerns arising from use of such specialized systems, which make their overall acceptability challengeable are highlighted. Section V highlights applicable existing measures and proffers newer measures to the issues identified earlier. Recommendations on future work are highlighted in the conclusion section.

2. METHODOLOGY

This paper is as a review article considered different resources and related reviews for investigation and analysis to provide a more concise and updated direction. Thus, related materials are collected from research repositories, and are provided in the chronological order of presented content. The materials are mainly concerned with the concepts, case studies, challenges, and opinions around the ethical usage of digital forensic systems. Each of the selected material covering a subset of these elements is ultimately matched together to provide a more complete and clearer picture, from which the most recurring factors are identified, and their contributions are subsequently discussed.

3. ETHICAL CONCERNS IN INFORMATION SYSTEMS

Issues arising from the development and implementation, particularly, of information systems are generally fitted under three major classes – technical, socio-economical and legal. However, it is not uncommon for certain issues to span across more than any one major class. A number of these concerns are briefly highlighted below.

3.1. Privacy and Confidentiality

Stakeholders' privacy had not been considered an important aspect of deployed information system processes until recently, even though it has always been a fundamental part of theoretical systems. However, the call for stakeholders' confidentiality has garnered momentum, pushing it to the top of the list of the most debated issues in information systems (Niemeijer, 2010); (Information Commissioner's Office, 2009). Sensitive and/or non-sensitive data of direct and indirect stakeholders flow through information systems in the process of producing tailored and informed decisions for individuals and their organizations respectively.

When mechanisms that ensure the confidentiality of data flowing through the systems are not put into place, such data become susceptible to unauthorized access by third parties as well as misuse by authorized parties (Rössler, 2005). Thereby, infringing the privileges of involved parties and leading to computer incidents including data breaches, identity crimes, intellectual property and trade secret thefts, and cyber warfare amongst others (Balogun & Zhu, 2013); (Home Office, 2003).

Although this issue borders on ethics, as the obligation of safeguarding stakeholder data from unapproved use was a non-mandatory requirement for information systems except of those organizations that valued morality. However, various legislations have since been formulated to address the ethical concerns in the usage of information systems. A typical example of such legal interventions is the UK Data Protection Act 1998 that ensures that individual and organizational data collected by organizations are used specifically for the purposes for which they were collected only (Rössler, 2005); (Information Commissioner's Office, 2009); (Balogun & Zhu, 2013). In spite of this, newer concerns arise with the rapidly advancing information technology than legal interventions have been able to keep up with. Thus, there is need for stop-gap measures to address ethical confidentiality concerns of stakeholders as soon as technological advancements induce them.

3.2. Repudiation and Obfuscation

Information systems encroach on every part of the setup it has been deployed to support. Every process and stage is transparent to the system in a bid to ensure it receives the relevant data to infer and recommend accurate trends and fixes respectively (Kubitschke, Gareis, Lull & Müller, 2009). Inputs are taken from various stages throughout the cycle of the setup to allow informed decisions to be made at the end of specified timelines or milestones. The inputs and feedbacks taken are usually untraceable further than department/level they came from, since anonymity is usually promised in a bid to encourage individual participants to provide accurate data (Kubitschke et al., 2009).

Consequently, short-term (day-to-day) decisions made at various levels become repudiatory, as the individual sources leading to them are difficult to trace. This allows for the absolution of decision-making employees from being held outrightly accountable for their organization’s mishaps, as they can repudiate their involvement in such incident since the system has obfuscated the unnecessary detail of its workings.

While the repudiation privilege afforded to employees as a result of the input anonymity and system process obfuscation is undesirable to organizations, it is unknown what organizations are prepared to do to mitigate damages resulting from anonymous employee inputs or actions. It has been suggested that organizations might consider tweaking their information systems to enable them

breach the anonymity clause and identify the employees to which certain inputs are attributed.

3.3. Accuracy and Efficiency

Information systems are adjudged as a more efficient decision support mechanism to large organizations than the traditional manual mechanism. While the manual mechanism might be efficient for small scale organizations that employ in units and generate data in megabytes, its efficiency becomes a challenge where larger organizations generate gigabytes or terabytes of data from hundreds of employees and thousands of customers. Sifting through such big data in order to identify trends and predict behaviours in real and minimum time possible is a task more appropriately handled by information systems, that has incomparably large processing capabilities to see the whole picture at any particular time.

However, the accuracy of information systems can pose a technical issue like any typical software based on the belief that an information system is only as accurate as the data fed to it and the intelligence of its developer (Bostrom, 2008); (Kubitschke et al., 2009). An inexact understanding of the organization's workflow by the developer of the information system would pose an inaccurate capturing of the picture needed to infer hypotheses (Ridder, 2009). Development and runtime bugs are unavoidable, and are usually identified as a result of numerous test-drives prior to deployment (Carrier, 2005); (Sheetz, 2007). However, they are still found in most running systems, compromising the accuracy and integrity of information systems and their results respectively.

The concern remains whether to knowingly deploy potentially-buggy information systems and provide fixes to them as soon as organizations detect them or to deploy information systems only after they have gone through exhaustive test-drives and certified bug-free, in order to ensure they provide only accurate results to support organizations' decisions that would affect their socio-economic fortunes.

3.4. Replacement and Reduction

As a result of the large processing capacity and automated operation that information systems are equipped with, their decision support analyses are faster and more accurate than obtainable from the traditional manual mechanisms. Subsequently, results from information systems are timelier and more cost-efficient for organization's long-term success.

This informs organizations' preference of deploying information systems rather than the manual mechanism for supporting organizational decision-making. Unfortunately, obsoleting the manual mechanism translates to rendering human employees surplus to such organizations' requirements (Kubitschke et al., 2009). Unemployment is a persistent socio-economic issue that virtually all countries are faced with, in varying degrees. An entire shift to information systems directly puts people whose job description have been partially or wholly automated out of their jobs (Borges, 2008); (Ho, Wheatley & Scialfa, 2005). Thus, a dilemma arises between the choices to maximize organizational turnover – one that benefits the organization, and to keep a workforce engaged – one that benefits the society.

3.5. Manipulation and Falsification

The use of information systems allow simultaneous and remote access to various forms of data and documents by employees and the general public, unlike the traditional manual mechanism. The ease of availability coupled with the easy manipulation promoted by information systems' techniques enable easier, faster and more accurate reproduction of data to fit the user's agenda (Bostrom, 2008).

While the original intention for information systems' manipulation techniques is to foster organizational efficiency, their use by parties motivated by illegal aims to advance unsavoury intentions continues to be a menace to the welfare of the society (Sheetz, 2007); (Marshall, 2008). Although there are continuous efforts to detect and control criminal and immoral manipulations (falsification), perpetrators still find creative ways to exercise unethical data/document falsification.

Thus, the challenge lies in whether to rid all information systems of manipulation techniques, to make the manipulation techniques available to select users with adequate checks to prevent their abuse, or to allow the existence of the manipulation techniques while exploring ways to keep up with detecting criminal falsifications.

4. INFORMATION SYSTEMS VS DIGITAL FORENSIC SYSTEMS

Although digital forensic systems are quite similar to information systems, and are as thus classified together, there are certain features that extend digital forensic systems from the typical information systems. The distinguishing characteristics that extend the digital forensic system from typical information systems classification are highlighted in this section.

4.1. Purpose and Functionality

Information systems are program suites that are designed for efficient performance of general tasks in a particular domain. These suites contain programs that have far-reaching functionality, usually often adaptable for use in other tasks than those they have been developed for. They are thus referred to as ad-hoc systems, because of their generally versatile nature.

However, digital forensic systems are suites that are designed for a singular purpose of conducting forensic investigations efficiently. Each program in the suites addresses a particular investigation subtask, and cannot be adapted for non-investigative purposes (Carrier, 2005); (Casey, 2009); (Volonino, Anzaldua & Godwin, 2007). Thus, digital forensic systems are specialized. While Microsoft Office Word can be used virtually across administrative, scientific, accounting, and other domains, the inbuilt word processor in Encase Forensic Reporter is automated to document investigation details alone and cannot be used separately for other purposes.

4.2. Availability and Pricing

Majority of the typical information systems that individuals and small/large organizations need to perform their day-to-day routine efficiently are easily and readily available for free or nominal fee. While alternatives exist abound, organizations might request an entirely customised information system from in-house or commercial developers.

However, digital forensic systems are required to perform tasks that are taken on or anticipated by large organizations, rather than individuals. Thus, their availability is restricted to private investigators, law enforcements and, to an extent, academia for research purpose. The costs of digital forensic systems are relatively high, and affordable to the large organizations only. The scarce availability of these systems is due to the sensitivity of the tasks they are developed for, as easy availability would open them up to reverse engineering and anti-forensic attacks (Beebe, 2009); (Casey, 2009).

4.3. Prerequisite Skill and Training Requirement

ICT practitioners are regarded as proficient in the domain, and as such are capable of properly using typical information systems with little or no training. The knowledge they have acquired from lessons and experiences are generally enough to implement typical information systems in sufficient levels.

Digital forensic systems, on the other hand, are more advanced information systems. One of the principles in the domain enforce its stakeholders to undergo proper training to certify them sufficient in the use of the system for its purpose efficiently. General information system knowledge is not accepted as sufficient to implement the digital forensic systems for critical organization or government business (Meyers & Rogers, 2004). Certain forensic skills are required as prerequisites for undergoing the training, and subsequently implanting the system independently. This is due to the intricacies involved in the use of the system, and the complexities associated with the system workings (Beebe, 2009).

4.4. Reliability and Admissibility Validation

Information systems are subjected to various testing during their development lifecycle. These pre-deployment tests are performed by the developers and are most likely to stop after the system has been deployed, except for the customized or subscription-based systems (Bianco, Lewis, Merson & Simanta, 2011). Validation of developer claims are rarely performed, except by few academia and/or individuals that need to confirm the suitability of such systems for their project requirements.

Digital forensic systems are subjected to a lot more field use than the tests claimed by their developers. The domain regulators and courts enforce the demonstration of the reliability of digital forensic systems used and the subsequent results they produce. Thus, digital forensic tools are subjects of thorough field tests across the industry, academia peer reviews and investigator benchmark tests, in addition to the developer tests in order to ascertain their accuracy and reliability for evidence admissibility (Guo, Slay & Beckett, 2009); (Wilsdon & Slay, 2005). This spells the amount of reliance on digital forensic systems, and the impact of their results on the social, economic and legal issues.

5. OPEN ETHICAL CONCERNS IN DIGITAL FORENSIC SYSTEMS

In this section, current issues arising from the development and implementation of digital forensic systems that are unaddressed are highlighted, with the expectation that future researches would be focussed on addressing the concerns they pose to the welfare of an automated modern society.

5.1. Fear of Unpredictability

Due to the complexities in the nature of digital artefacts from which evidences are gathered, various digital forensic tools exploit various techniques to perform the

same tasks (Casey, 2009). Although the use of different techniques is adjudged to help investigators to keep up with containing new ways of misusing information systems efficiently (Volonino et al., 2007), it becomes confusing to users which computing behaviours are deemed inappropriate by which digital forensic tools.

The resultant fear tends to influence the computing activities of users, as they become conservative rather than expressive (Kubitschke, 2009). This can affect the quality of feedbacks being supplied by the users to the system, and the accuracy of the system in detecting trends of computer usage is impaired.

5.2. Breach of Privacy

The recommendation that disk manufacturers should provide backdoors to aid investigators to bypass lockouts and ensure effective digital forensic analyses has gained proponents who has argued for its commercial implementation (Balogun & Zhu, 2013). In the same vein, digital forensic systems employ backdoor entry techniques to user devices for collection of potential evidential data.

The potential access these techniques grant to a certain group – supposedly law enforcement – to individual/organization's non-public information poses a serious moral concern. In addition to that, there is a genuine possibility that such techniques would find their way into the wrong hands, who would breach the confidentialities attached in infringing and embarrassing manners.

5.3. Exploitation of Tools

The functionality of digital forensic systems are unique and straightforward. However, experienced computer users with certain skillsets can reverse engineer or extend modules of a digital forensic system – especially open source systems that grant such permissions – for personal use (Fitzgerald, 2006); (Ridder, 2009). These tools are even used to frustrate their own effectiveness in anti-forensic moves, thus discrediting the information they produce as results.

Thus, questions arise about how open source digital forensic systems can be prevented from being exploited for unethical use, and how their exploited implementation instances could be detected. Other concerns arise about the open licence nature of some digital forensic systems, and whether it is more secure to make all digital forensic systems proprietary to inhibit immoral exploitations.

Vol 9, No 1, 2017 ISSN: 2146-0744 (Online)

5.4. Commercial and Market Share Motives

The digital forensic system market is not as competitive as the typical information system market. Unlike the latter, the earliest developers in the former market have acquired and still retain the majority of the market share. This could be attributed to the relative immaturity of the digital forensics discipline, and the fact that such developer reputations earned from the legal systems serve as precedents that do not change very often (Casey, 2009).

Yet, digital forensic system developers show virtually no proof to the claims about the accuracy and reliability of their systems. Investigators take these claims at face value, and tend to prefer the earliest developers due to their reputations. However, the possibility that these revered developers hype their systems more than their actual capabilities, in the bid to retain or acquire larger share of the market, exists (Balogun & Zuva, 2017). It also hinders the market share index and implementation of more efficient digital forensic systems and discourages better digital forensic investigation process in the long run.

5.5. Standardization of Practices

The difference in the nature of practice, in which information system practices are more straightforward than the practices in the digital forensic domain, is a persistent issue worth mentioning. Users of digital forensic systems always rely on experience and creativity in setting up procedures to complete tasks, whereas typical information system users use clearly set out procedures (Casey, 2009). Though standardization of digital forensic system implementation has been attempted and revisited often, its actualization has been elusive (Garfinkel, 2010).

Thus, it remains unclear how to determine whether all procedural variations of digital forensic system practices are effective, or which among them is the most efficient for recommendation as a standard.

5.6. Inconsistent Educational/Training Outcomes

As mentioned in the previous section, the use of digital forensic systems require prerequisite specialized skills. These skills are not acquirable from general computing education which are usually enough to use typical information systems. They are imparted through specific education or training over a period of time by academic universities and professional organizations, in formal and informal modes.

However, there are significant differences in the quality and quantity of skills learnt at various training centre due to a lack of regulation. As a result, there are concerns about the sufficiency of specialized skills claimed by users of digital forensic systems as well as the accuracy of the results they arrive at (Meyers & Rogers, 2004). There are also concerns about the specific set of academic and/or professional qualifications or skills that are necessary to prove that a person is adequately competent enough to take up certain positions in which they would use certain digital forensic systems (Wilsdon & Slay, 2005).

6. MEASURES FOR IDENTIFIED CONCERNS

This section highlights the applicable measures that are currently in place for the issues identified in the previous section. Probable measures are also proffered where existing measures are lacking.

6.1. Legal Measures

While a particular society's legislations have always been used instead of its ethical principles to remedy issues with serious consequences within it (Lynch, 1994), there have been issues which legislation takes too long to intervene in or could not intervene in at all due to technical or geographical complexities.

However, it could be argued that the slow pace at which legislative frameworks intervene is due to the obligation to ensure that all considerations are taken for the eventual laws to be effective. The long-term effectiveness of laws against ethical information system concerns is relatively dependent on technical understanding of the said issue. The more complex and rapidly-changing nature of digital forensic systems could make legal interventions even slower, and only effective when enacted properly. Examples of these legislations include the UK Data Protection Act, the European Data Protection Directive, the Scotland Regulation of Care Act, the Financial Services Act, as well as in the United National Universal Declaration of Human Rights, the European Convention on Human Rights, and the European Convention on Human Rights. Constant review of such legislative frameworks is necessary to address the legal gaps and keep up with the rapid-changing nature of digital forensic systems.

Thus, improved collaboration among the legal arm and the digital forensic system stakeholders would foster the understanding sufficient to enact and enforce laws that would tackle the identified ethical issues in faster times, in order to keep the

society safe from the negatives of digital forensic systems while reaping the positives.

6.2. Technical Measures

Legal measures have been unable to resolve some ethical issues induced by digital forensic systems. This is usually because the ethical principle(s) outlining such issues are not strong enough to instigate a legislative process. Thus, such ethical issues are resolved by technical interventions.

6.2.1 Training

Ensuring the training of the users of digital forensic systems is a reactive way to tackle the associated ethical issues. It imparts the users with prerequisite specialized skills necessary to prevent such ethical issues identified from occurring as a result of their actions.

However, it would be more appropriate that such trainings are handled by the digital forensic system vendors, because of their privileged knowledge about the system workings over typical academic and/or professional trainers.

6.2.2 Redevelopment and Restucturing

Another measure in the technical domain is the redevelopment of digital forensic systems, which is a rather proactive move. Once the ethical issues identified have been translated into requirements specification, a refined digital forensic system or a refined digital forensic process – as the case may be – would tackle the ethical issues that are rather due to technical reasons than legal or cultural reasons.

7. CONCLUSION

The existence of ethical issues, as the compromises of the success of computing technology, has been established. The similarities of digital forensic systems to typical information systems, as well as their distinctions, have been discussed. Although both classes tend to be burdened with similar societal concerns, digital forensic systems have much more issues due to factors such as their infancy and specialization, amongst others.

This paper has identified and highlighted the ethical issues that remain to be resolved within the development and implementation of digital forensic systems in the society. It harbours the platform that future studies, which would focus on finding appropriate resolutions to each of the issues highlighted in this paper, would build on.

REFERENCES

Balogun, A. & Zhu, S. (2013). Privacy Impacts of Data Encryption on the Efficiency of Digital Forensics Technology. International Journal of Advanced Computer Science & Applications, 4(5), 36-40.

Balogun, A. & Zuva, T. (2017). Open Issues in Cybercriminal Profiling. Proceedings of the 1st IEEE Next Generation Computing and Applications Conference, Mauritius, 1(4), 1-5.

Balogun, A. & Zuva, T. (2017). Towards the Adoption of Software Engineering Principles for Assessing and Ensuring the Reliability of Digital Forensic Tools. ", In: R. Silhavy P. Silhavy & Z. Prokopova. (eds.), Cybernetics Approaches in Intelligent Systems. CoMeSySo 2017. Advances in Intelligent Systems & Computing, Vol 661, Springer, Cham, Pp 271-282.

Baqgini, J. & Fosl, P. (2007). The Ethics Toolkit: A Compendium of Ethical Concepts and Methods. Malden: Blackwell.

Beebe, N. (2009). The Good, The Bad, and the Unaddressed. Fifth IFIP International Conference of Digital Forensics, Orlando, Florida; USA, 17-36.

Bianco, P., Lewis, G., Merson, P. & Simanta, S. (2011). Architecting Service-Oriented Systems. Software Engineering Institute, Carnegie Mellon University, 1-36.

Borges, I. (2008). Older people and information and communication technologies – an ethical approach, AGE.

Bostrom, N. (2008). Dignity and enhancement, Institute for Emerging Ethics and Technologies.

Carrier, B. (2005). File System Forensic Analysis. Upper Saddle River, NJ: Addison-Wesley.

Casey, E. (2009). Handbook of Digital Forensics and Investigations. Elsevier Academic Press, London.

Fitzgerald, B. (2006). The Transformation of Open-Source Software. MIS Quarterly, 30(3), 587-598.

Garfinkel, S. (2010). Digital Forensics Research: The Next 10 Years. Digital Investigation, 7, s64-73.

Guo, Y., Slay, J. & Beckett, J. (2009). Validation and verification of computer forensic software tools – Searching Function. Digital Investigation, 6, s12-s22.

Ho, G., Wheatley, D. & Scialfa, C. (2005). Age differences in trust and reliance of a medication management system. Interfacing with Computers, 17, 690-710.

Kubitschke, L., Gareis, K., Lull, F. & Müller, S. (2009). ICT & Ageing: Users, markets and technologies: compilation report on ethical issues, unpublished report.

Lynch, M. (1994). Ethical Issues in Electronic Information Systems. The Geographer's Craft. http://www.colorado.edu/geography/gcraft/notes/ethics/ethics_f.html. Accessed 2017/07/15.

Marshall, A. (2008). Digital Forensics: Digital Evidence in Criminal Investigations. Hoboken, New Jersey: Wiley-Blackwell.

Meyers, M. & Rogers, M. (2004). Computer forensics: The need for standardization and certification. International Journal of Digital Evidence, 3(2), 1-11.

Miller, C. (2009). The Conditions of Moral Realism. The Journal of Philosophical Research, 34, 123-155.

Mohay, G., Anderson, A., Collie, B., Vel, O. D. & Mckemmish, R. (2003). Computer and Intrusion Forensics. Artech House Inc.

Niemeijer, A. (2010), Information/opinion provided in the framework of Alzheimer's Europe's Dementia Ethics Network project on the ethical use of assistive technology by/for people with dementia.

Ridder, C. (2009). Evidentiary Implications of Potential Security Weaknesses in Forensic Software. International Journal of Digital Crime and Forensics, 1(3), 80-91.

Rössler, B. (2005). The value of privacy. Cambridge, MA: Cambridge University Press.

Sheetz, M. (2007). (2007). Computer Forensics: An Essential Guide for Accountants, Lawyers and Managers. Florida: John Wiley & Sons.

Shinder, D. (2005). Ethical issues for IT security professionals. http://www.computerworld.com/article/2557944/security0/ethical-issues-for-it-security-professionals.html. Accessed 2017/07/20.

Volonino, L., Anzaldua, R. & Godwin, J. (2007). Computer Forensics: Principles and Practices. Upper Saddle River, New Jersey: Pearson Education Inc.

Wilsdon, T. & Slay, J. (2005). Digital forensics: Exploring validation, verification and certification. Proceedings of the first International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE), Washington, DC, 48-55.