Chapter 11

A FORENSIC FRAMEWORK FOR HANDLING INFORMATION PRIVACY INCIDENTS

Kamil Reddy and Hein Venter

Abstract This paper presents a framework designed to assist enterprises in implementing a forensic readiness capability for information privacy incidents. In particular, the framework provides guidance for specifying high-level policies, business processes and organizational functions, and for determining the device-level forensic procedures, standards and processes required to handle information privacy incidents.

Keywords: Forensic readiness capability, information privacy incidents

1. Introduction

Information privacy is the interest individuals have in accessing, controlling or influencing the use of their personal information [7]. The protection of information privacy is mandated by law in many countries [16, 20]. Enterprises operating in these countries have a legal obligation to secure the information they use. Over and above the legal obligations, consumers [11] and corporate governance standards [12] demand that information privacy be protected regardless of the geographical location of an enterprise.

Digital forensic readiness is a corporate goal involving technical and non-technical actions that maximize the ability of an enterprise to use digital evidence [19]. It ensures the best possible response to incidents that may occur in an enterprise network. Maintaining an effective forensic readiness capability requires carefully considered and coordinated participation by individuals and departments throughout the enterprise [19]. A forensic readiness capability developed or executed in an *ad hoc* manner is unlikely to succeed [8].

The concepts of information privacy and forensic readiness intersect when an information privacy violation occurs and it is necessary to conduct a forensic investigation of the violation. While privacy violations are often the result of security breaches (e.g., unauthorized access to private information), they also occur when private information is used inappropriately by individuals who are authorized to access the information. Therefore, enterprises with a forensic readiness capability for dealing with security-related incidents may not be in an optimal position to respond to privacy-related incidents. To address this issue, we propose a framework that considers the requirements for ensuring forensic readiness with respect to information privacy incidents.

The framework is a theoretical representation of a generic forensic readiness capability for dealing with information privacy violations in an enterprise. As such, it aims to provide a basis upon which enterprises can build a forensic readiness capability for information privacy incidents. Since forensic readiness requires the participation of individuals at all levels and across departmental boundaries [19], the purpose of the framework is to provide guidance at a high level by specifying the appropriate policies, business processes and organizational functions. It also enables an enterprise to determine the device-level forensic procedures, standards and processes required to implement a forensic readiness capability for information privacy incidents.

It is important to note that this paper focuses on the structural aspects of the framework rather than its procedural aspects. Structural aspects refer to the choice of the elements contained in the framework and the relationships between the elements. On the other hand, the procedural aspects merely deal with the practical measures necessary to implement the framework in an enterprise. To our knowledge, little, if any, research focusing on the structural aspects of a forensic readiness framework for handling information privacy incidents has been published.

2. Related Work

This section discusses related work on forensic readiness and the role of information privacy in digital forensics. It also discusses the "Fair Information Principles" [9], which are at the core of most approaches for protecting information privacy.

The work of Endicott-Popovsky, *et al.* [8] focuses on forensic readiness at the enterprise level. It deals with network forensic readiness as a means for breaking the cycle of attack and defense. Our work is different in that it also addresses information privacy and includes a wider variety of information technologies and business processes.

Other efforts related to forensic readiness have concentrated on tools and techniques [8]. Several researchers have focused on the organizational aspects of forensic readiness. Yasinsac and Manzano [23] have defined policies for computer and network forensics; Wolfe [23] has discussed forensic policies in organizations; Rowlingson [19] has specified a ten step process for implementing forensic readiness; Luoma [13] has proposed the establishment of a multi-disciplinary management team to ensure legal compliance with discovery requests; and Taylor, *et al.* [21] have studied forensic policy specification and its use in forensic readiness.

The vast majority of work related to privacy in the digital forensic literature focuses on protecting the privacy of computer users during forensic investigations [1, 2, 4]. Unfortunately, a comprehensive treatment of information privacy and its impact on forensic readiness has not been conducted.

The Fair Information Principles are a guide for the ethical handling of private information and form the basis for information privacy laws in countries around the world [9]. The eight principles, as espoused by the Organization for Economic Cooperation and Development [17], are: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability. The principles provide a practical definition of information privacy and specify obligations for enterprises with regard to the ethical handling of private information. In addition to covering information privacy, the obligations focus on protecting the confidentiality of data subjects. Enterprises that fail to meet these obligations are likely to be in violation of information privacy laws.

3. Rationale

Information security has traditionally been concerned with the confidentiality, integrity and availability of information [21]. Information privacy, on the other hand, focuses on the ethical and legal use of information [3]. Confidentiality, integrity and availability are necessary – but insufficient – conditions for information privacy [3]. Thus, information privacy has a wider range of potential violations and incidents since the ethical and legal use requirements are in addition to the traditional requirements for security.

Ethical or legal usage requirements related to information privacy directly affect enterprise business processes. Businesses processes do not specify the boundaries for acceptable use. Ideally, acceptable use is specified via policies [21] derived from authoritative sources such as information privacy laws and ethical guidelines. In some instances, eth-

ical guidelines (such as the Fair Information Principles) may require the creation of "privacy-specific business processes" that deal with private information. An example is a business process that handles requests to access information.

Information technology underlies privacy-related and privacy-specific business processes. In an enterprise, information technology facilitates the execution of business processes that operate on private information. The particular information technologies used in a business process determine to a large extent what can be done with private information. For example, using a database instead of flat text files, makes it easier to query the stored data. Therefore, policies are required to govern the use and configuration of information technologies to ensure that they are used appropriately.

Digital forensic investigations of information privacy incidents in an enterprise involve the information privacy context: privacy-related business processes, privacy-specific business processes, information technologies supporting the processes, policies that govern the processes, and the auditing and monitoring of processes. The information privacy context, with the exception of information technology, expresses what is required by a privacy-specific approach for digital forensic readiness in addition to the traditional security-related approach.

There are two cases in which a forensic readiness capability for information privacy incidents is particularly useful. The first occurs when an entity outside the enterprise violates a subject's information privacy; this situation closely parallels the common security-related scenario of an outsider attacking the enterprise. The second case is internal in nature. An example is when a data subject alleges that the enterprise itself is responsible for the information privacy violation. If the data subject takes legal action, a forensic readiness capability for information privacy incidents would enable the enterprise to conduct an effective digital forensic investigation that can be used in its defense. Another example is when an employee is charged with violating the enterprise's privacy policy. The enterprise may conduct a digital forensic investigation to present evidence against the employee in a disciplinary hearing. The investigation is likely to proceed very efficiently if the enterprise has a mature forensic readiness capability for information privacy incidents.

4. Forensic Framework

This section describes the framework intended to provide enterprises with a generic forensic readiness capability for dealing with information

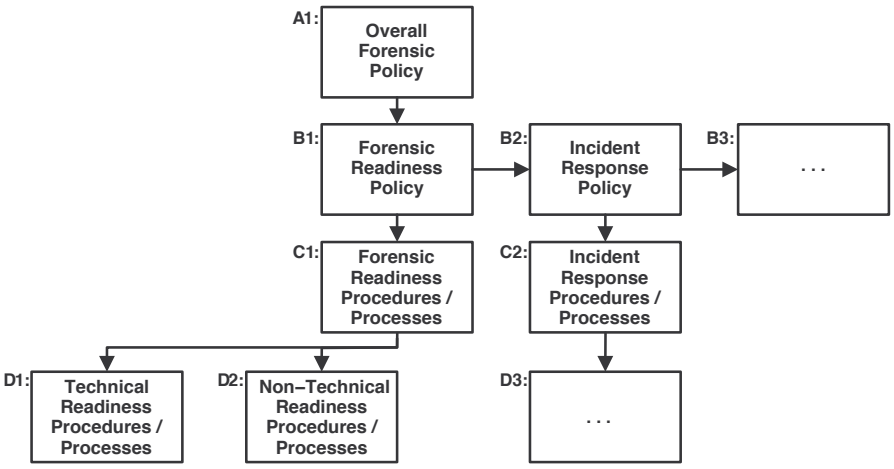

Figure 1. Forensic framework (Levels A – D).

privacy incidents. Due to the size of the framework, we only examine the components that are relevant to handling information privacy incidents.

The forensic framework has a hierarchical tree-like structure with several levels (Figure 1). Each level has various elements depicted as blocks. The blocks within a level (e.g., Level B) are labeled sequentially from left to right (e.g., Blocks B1, B2 and B3).

4.1 Top Levels

At the top of the framework is Block A1, which corresponds to an overall forensic policy that has been approved by management. The forensic policy guides the processes and procedures involved in digital forensic investigations [15, 22]. It also provides official recognition of the role of digital forensics in the enterprise [22].

Block A1 is decomposed into several Level B blocks, each of which represents a phase in the digital forensic investigation model of Carrier and Spafford [6]. The phases are incorporated in the framework to highlight the fact that a forensic policy must cover all the investigative phases. Since the focus is on forensic readiness, we only list the incident response phase (Block B2). It is important to note that the decomposition from Level A to Level B is logical, not physical. Thus, each phase of a digital forensic investigation does not require a separate policy; for example, all the phases may be addressed using a single forensic policy (i.e., the overall policy).

The policy in Level B is implemented as procedures or processes in Level C (Figure 1). Because of the focus on digital forensic readiness,

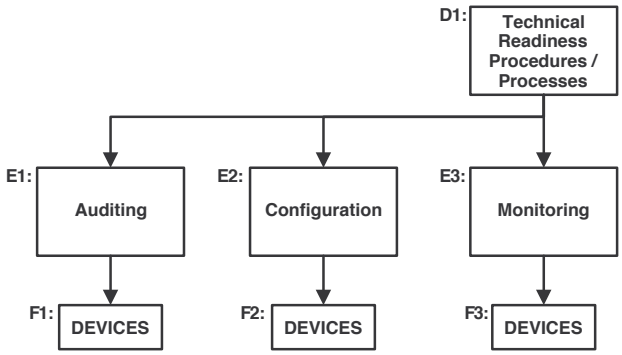

Figure 2. Technical components (Levels D – F).

we only follow the branches leading from Block C1. Block C1 expands to Block D1 (technical readiness procedures and processes) and Block D2 (non-technical readiness procedures and processes).

4.2 Technical Readiness Components

Blocks D1 and D2 represent the technical and non-technical components of digital forensic readiness. According to Rowlingson [19], monitoring and auditing are important components of digital forensic readiness because they help detect and deter incidents. Additionally, procedures and processes must be in place to retrieve and preserve data in an appropriate manner. This is modeled by splitting Block D1 into Blocks E1 through E3 (Figure 2).

Block E2 covers configuration standards, procedures and processes. Blocks E1 and E3 (auditing and monitoring) depend on what is identified under Block E3, and may not be possible unless the hardware and software are configured properly. Consider, for example, two cases: (i) a firewall is not configured to log certain events, and (ii) a firewall and switch are both configured to log events, but are configured to use different time servers. In the first case, events that are not logged by the firewall will not be observed by the monitoring and auditing processes. In the second case, it may be difficult to correlate events from the switch and firewall, which reduces the evidentiary value of the logs that are produced.

Blocks F1 through F3 denote the monitoring, auditing and configuration devices (hardware, software and policy) used in the appropriate business process.

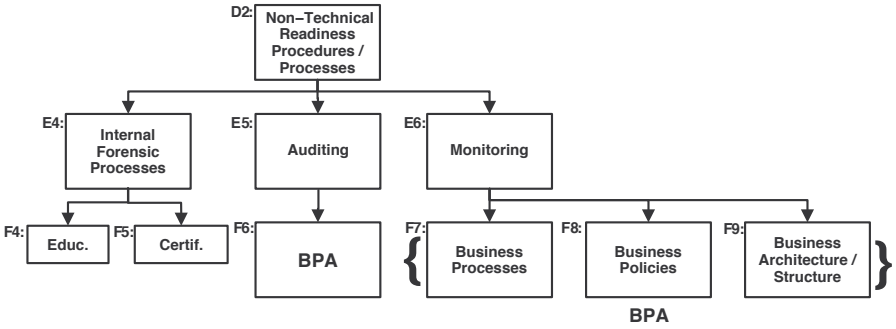

Figure 3. Non-technical components (Levels D – F).

4.3 Non-Technical Readiness Components

The branches from Block D2 in Figure 3 are concerned with the non-technical aspects of digital forensic readiness. Many of the forensic readiness aspects pertinent to privacy are found in this part of the framework. The non-technical components of the framework comprise internal forensic processes, auditing and monitoring (Blocks E4 through E6).

The internal forensic processes in Block E4 are processes that are unique to the forensic team of an enterprise. An example of such a process is the education [14] of forensic team members (Block F4). When implementing a forensic readiness capability for information privacy incidents, it is important to educate forensic investigators (who are primarily trained in security) about information privacy laws. Forensic team members should also have the appropriate certifications (Block F5). These include certifications for conducting digital forensic investigations as well as privacy-related certifications [10].

Blocks E5 and E6 refer to the auditing and monitoring of business processes, policies and architecture. The business processes and policies are those that have relevance to information privacy in the enterprise. Likewise, the business architecture is limited to the structure of the business as it pertains to information privacy. Examples include the creation of a chief privacy officer (CPO) and the creation of a multi-disciplinary team [13] consisting of staff from the office of the CPO, information security, forensics and legal departments. Blocks F7 through F9 correspond to business processes, policies and architecture, respectively. Block F6 expresses the interactions and impact of the business processes, policies and architecture.

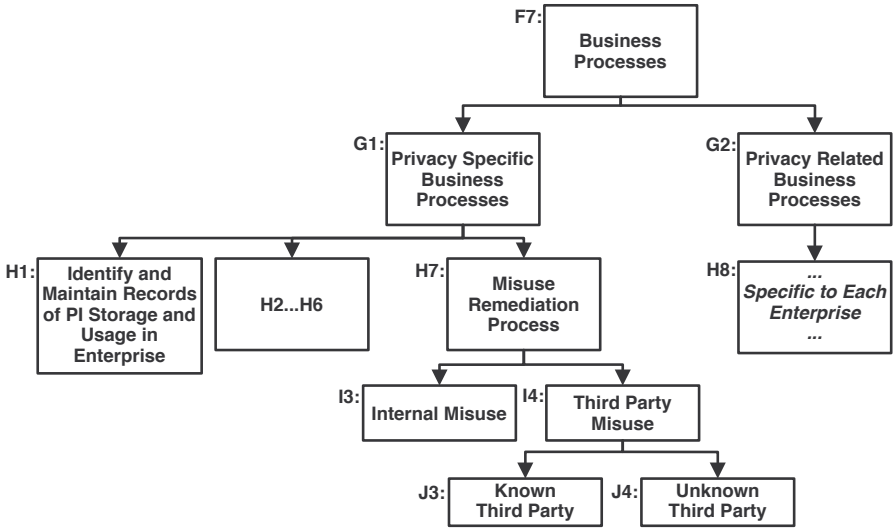

Figure 4. Business processes.

Privacy and Business Processes

Figure 4 shows the decomposition of business processes into privacy-specific and privacy-related business processes from Block F7 to Blocks G1 and G2. Block G2 is an abbreviation of these processes since they are unique to each enterprise and depend largely on the nature of the enterprise. For example, in a delivery company, the process of capturing the details of a delivery to a client is considered to be a privacy-related process because the client's address is private information. Including privacy-related processes in the framework is important because it gives digital forensic investigators immediate information about the business processes likely to be involved in privacy incidents.

Privacy-specific business processes, on the other hand, are processes that deal purely with information privacy. They ensure that the actions required to protect information privacy and enforce the privacy rights of data subjects are in place within the enterprise. The processes are shown as branches of Block G1 in Figure 4. The following processes are omitted to save space: process for communicating the privacy policy (Block H2), process for aligning the privacy policy with business policies (Block H3), process for handling requests to access private information (Block H4), process for correcting private information (Block H5), and process for complaints and complaint escalation (Block H6).

The privacy-specific business processes in the framework are taken from the Generally Accepted Privacy Practices (GAPP) Standard [5].

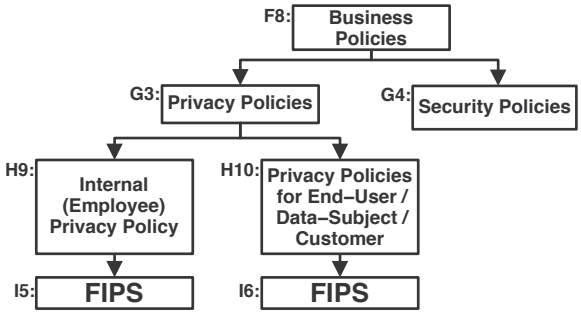

Figure 5. Privacy policies.

Block H7 (misuse remediation process) is used as an example of the many privacy-specific business processes. Misuse remediation describes incidents in which private information is used in a manner that has not been sanctioned by the data subject. Misuse is divided into internal misuse and third party misuse, expressed using Blocks I3 and I4, respectively. The delineation provides for the different digital forensic readiness processes that may be required for each category and sub-category. For example a readiness process for handling privacy incidents with a business partner may include the establishment of a joint forensic team at the outset of the partnership.

Privacy Policies

Figure 5 shows the information privacy policies of an enterprise. Privacy policies in the framework are split into an internal privacy policy for employees of the enterprise (Block H9) and privacy policies for data subjects (Block H10). The internal privacy policy defines guidelines for the acceptable use of private information (belonging to data subjects) by employees. As such, it plays an important role in defining an information privacy incident because an incident usually occurs when the policy has been violated by an employee. It also clarifies the repercussions for employees if they do not adhere to the guidelines.

Privacy policies for data subjects also inform data subjects about the enterprise's practices regarding their private information. Data subjects may then hold an enterprise to the policies and can institute complaints when they believe that the enterprise has not adhered to the policies. The policies are clearly very useful to a forensic investigator tasked with investigating a complaint by a data subject.

In the forensic framework, the internal privacy policy and the privacy policies for data subjects are based on the Fair Information Principles

(FIPS) that underlie most information privacy laws [9]. Other guidelines (e.g., applicable laws) may also be included in Blocks I5 and I6.

5. Discussion

One of the primary goals in the design of the framework is the inclusion of information privacy protection in the forensic readiness capability of an enterprise. Following the accepted notion that security-related forensic readiness is not possible unless basic information security processes (e.g., logging and incident reporting) are in place [8, 22], we hold that the same is true for a forensic readiness capability for information privacy incidents. An enterprise must implement information privacy practices to maintain a forensic readiness capability for information privacy incidents. The GAPP Standard [5] is used to incorporate specific measures for protecting information privacy within the framework. Enterprises with higher levels of maturity regarding information privacy protection are more likely to have better forensic readiness capabilities for information privacy incidents than those with lower levels of maturity [18].

The framework also incorporates established concepts from security-related forensic readiness [8, 19, 22, 23], namely a policy and a process approach to forensic readiness. Indeed, the primary contributions are the combination of these established concepts with information privacy protection measures and the definition of the relation between the policies, processes and procedures with respect to information privacy incidents. While the principal goal is the inclusion of information privacy protection in the forensic readiness capability of an enterprise, the framework itself is intended to serve as a theoretical guide for developing a forensic readiness capability for information privacy incidents. It is unlikely that the theoretical framework would be implemented "as is" in a real-world enterprise. Policies and processes that exist as separate elements in the framework may be combined if they already exist in an enterprise. Also, an enterprise may omit certain policies and processes. However, this introduces a risk in that certain aspects of information privacy protection may not be covered by the readiness capability. Risk and cost-benefit analyses [19] may be used to determine which, if any, items could be excluded.

A similar exercise to the mapping of technologies to business processes can be conducted with privacy policies and privacy-specific business processes. This could ensure that a digital forensic investigator knows which policies are relevant to incidents that involve specific business processes.

6. Conclusions

The digital forensic readiness framework for information privacy incidents is motivated by previous work on digital forensic readiness that identifies the need for policies, procedures and processes. It also encompasses information privacy imperatives by drawing on the Fair Information Principles, the GAPP Standard and the information privacy literature. The framework blends concepts from digital forensic readiness and information privacy to provide the essential elements for conducting digital forensic investigations of information privacy incidents. In particular, it provides enterprises with guidance for specifying high-level policies, business processes and organizational functions, and for determining the device-level forensic procedures, standards and processes required to implement a forensic readiness capability for information privacy incidents.

Our future work will refine the framework based on feedback from enterprises with mature forensic readiness capabilities. In addition, an ontology will be used to capture the relationships between framework elements and support automated reasoning.

References

[1] G. Antoniou, L. Sterling, S. Gritzalis and P. Udaya, Privacy and forensics investigation process: The ERPINA protocol, *Computer Standards and Interfaces*, vol. 30(4), pp. 229–236, 2008.

[2] H. Berghel, BRAP forensics, *Communications of the ACM*, vol. 51(6), pp. 15–20, 2008.

[3] H. Burkert, Privacy-enhancing technologies: Typology, critique, vision, in *Technology and Privacy: The New Landscape*, P. Agre and M. Rotenberg (Eds.), MIT Press, Cambridge, Massachusetts, pp. 125–142, 1997.

[4] M. Caloyannides, *Privacy Protection and Computer Forensics*, Artech House, Norwood, Massachusetts, 2004.

[5] Canadian Institute of Chartered Accountants, Generally Accepted Privacy Principles, Toronto, Canada (www.cica.ca/index.cfm/ci_id/258/la_id/1.htm).

[6] B. Carrier and E. Spafford, An event-based digital forensic investigation framework, *Proceedings of the Fourth Digital Forensic Research Workshop*, 2004.

[7] R. Clarke, Introduction to Dataveillance and Information Privacy and Definitions of Terms, Xamax Consultancy, Chapman, Australia (www.rogerclarke.com/DV/Intro.html), 2006.

[8] B. Endicott-Popovsky, D. Frincke and C. Taylor, A theoretical framework for organizational network forensic readiness, *Journal of Computers*, vol. 2(3), pp. 1–11, 2007.

[9] R. Gellman, Does privacy law work? in *Technology and Privacy: The New Landscape*, P. Agre and M. Rotenberg (Eds.), MIT Press, Cambridge, Massachusetts, pp. 193–218, 1997.

[10] International Association of Privacy Professionals, IAPP Privacy Certification, York, Maine (www.privacyassociation.org/index.php?option=com_content&task=view&id=17&Itemid=80).

[11] Y. Jordaan, South African Consumers' Information Privacy Concerns: An Investigation in a Commercial Environment, Ph.D. Thesis, Department of Marketing and Communication Management, University of Pretoria, Pretoria, South Africa, 2003.

[12] S. Lau, Good privacy practices and good corporate governance – Hong Kong experience, *Proceedings of the Twenty-Third International Conference of Data Protection Commissioners*, 2001.

[13] V. Luoma, Computer forensics and electronic discovery: The new management challenge, *Computers and Security*, vol. 25(2), pp. 91–96, 2006.

[14] G. Mohay, Technical challenges and directions for digital forensics, *Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering*, pp. 155–161, 2005.

[15] M. Noblett, M. Pollitt and L. Presley, Recovering and examining computer forensic evidence, *Forensic Science Communications*, vol. 2(4), 2000.

[16] A. Oliver-Lalana, Consent as a threat: A critical approach to privacy negotiation in e-commerce practices, *Proceedings of the First International Conference on Trust and Privacy in Digital Business*, pp. 110–119, 2004.

[17] Organization for Economic Cooperation and Development, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Paris, France (www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html).

[18] K. Reddy and H. Venter, Privacy Capability Maturity Models within telecommunications organizations, *Proceedings of the Southern African Telecommunication Networks and Applications Conference*, 2007.

[19] R. Rowlingson, A ten step process for forensic readiness, *International Journal of Digital Evidence*, vol. 2(3), 2004.

[20] South African Law Reform Commission, Privacy and Data Protection, Discussion Paper 109, Project 124, Pretoria, South Africa (www.doj.gov.za/salrc/dpapers.htm), 2005.

[21] C. Taylor, B. Endicott-Popovsky and D. Frincke, Specifying digital forensics: A forensics policy approach, *Digital Investigation*, vol. 4(S1), pp. 101–104, 2007.

[22] H. Wolf, The question of organizational forensic policy, *Computer Fraud and Security*, vol. 2004(6), pp. 13–14, 2004.

[23] A. Yasinsac and Y. Manzano, Policies to enhance computer and network forensics, *Proceedings of the Second IEEE Workshop on Information Assurance and Security*, pp. 289–295, 2001.