

Privacy Capability Maturity Models within Telecommunications Organisations

Kamil Reddy, H.S. Venter
{kreddy, hventer}@cs.up.ac.za

Information and Computer Security Architectures Research Group
Department of Computer Science,
University of Pretoria

Abstract—This paper discusses the problem of implementing information privacy protection at large organisations, particularly telecommunication service providers. It argues that implementation of organisation-wide information privacy protection is not solely a technical challenge but that, in order to be effective, organisational context also needs to be considered. In order to address organisational context, policies, processes and people must be taken into account. It is shown that privacy capability maturity models (PCMMs) are particularly well suited to doing this. This paper also addresses the absence of detail with regard to PCMMs by providing a description of the essential elements of PCMMs. Through a classification of privacy enhancing technologies (PETs), it further shows that PCMMs, together with what we term application-level organisational PETs, provide an optimal solution to the problem.

Index Terms— capability maturity model, information privacy, organisational privacy, privacy capability maturity model.

I. INTRODUCTION

Recent advances in information technology have enabled the unprecedented storage, access and transmission of information about individuals [4]. In countries, such as South Africa, which recognise and uphold the individual's right to privacy [7], it is usually accepted that this right allows the individual a certain measure of access to this information and control over its veracity and dissemination. The interest individuals have in controlling, or at least significantly influencing, the handling of information about themselves is termed *information privacy* [5]. The protection of information privacy has received increased attention as technological advances have made it easier to subvert information privacy. This increased attention is evident in proposed law such as the draft Bill on the Protection of Personal Information (Privacy Bill) [9]. The Privacy Bill, together with consumer demands for privacy [18] and the dictates of good corporate governance [20] mean that there is a strong imperative for large organisations

such as telecommunication service providers to consider information privacy issues. In a 2006 international survey of security in technology, media and telecommunications companies [22], 74% of respondents indicated that they “expect to spend more time in the coming year on information security due to governance and privacy regulations”. South African telecommunication service providers are under added pressure from sections 39 and 40 of the Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) [24], which, if enforced, would dramatically increase the amount of personal information they hold.

This paper therefore addresses the problem of finding an appropriate mechanism that telecommunication service providers can use to implement organisation-wide information privacy. It also addresses a current lack of detail on privacy capability maturity models (PCMMs) identified in the literature.

In light of the problem of dealing with information privacy, we propose that PCMMs are an effective way to implement organisational information privacy protection at telecommunication service providers. We argue that the adequate protection of information privacy within an organisation is not simply a technical challenge, but that it requires consideration of policies, processes, and personnel in an organisation.

Since PCMMs are mentioned but not elaborated on in detail in the literature, we describe the essential elements of PCMMs in Section II. We also classify privacy enhancing technologies (PETs) for the purpose of our argument in Section II. In Section III we describe what is necessary to fully develop a PCMM. In Section IV we demonstrate why policies, processes, and people need to be taken into account and why PCMMs, together with what we term application-level organisational PETs, are an optimal way of ensuring information privacy protection in organisations. We conclude in Section V and discuss future work.

II. BACKGROUND

In this section we present necessary background information on capability maturity models (CMMs), PCMMs, and PETs as a prelude to our advocacy of PCMMs as a means of protecting information privacy.

A. Privacy Capability Maturity Models

A privacy capability maturity model is a sub-class of the class of models known as capability maturity models (CMMs). As their name suggests, CMMs [3] [16] [17] are used by organisations to assess how mature their capability to perform certain organisational functions is. Information security and software engineering are two examples of such organisational functions. CMMs define *process areas* that are associated with the organisational function, and, in turn, define *practices*, or activities, that are usually involved in these process areas. The practices usually have *work products* associated with them. Work products may include reports, data or other documents that result from the practices. We use an example from the Systems Security Engineering Capability Maturity Model (SSE-CMM) [16] to illustrate this. The SSE-CMM defines a process area called

TABLE I
EXAMPLE PCMM PROCESS AREAS AND PRACTICES

Process Area	Practices
Assess Privacy Risks	<ul style="list-style-type: none"> Select the methods, techniques, criteria (e.g. legislation / fair information practices) by which privacy risks to the organization and data subjects are analysed, assessed, and compared. Identify all privacy risks to data subjects. Prioritise privacy risks. Monitor ongoing changes to the risks identified risks.
Manage and Administer	<ul style="list-style-type: none"> Develop and approve privacy policies, procedures, controls, and service level agreements. Communicate policies within the organization. Assign responsibilities for privacy practices. Review existing infrastructure, systems, applications, web-sites and remediate where necessary.
Monitor	<ul style="list-style-type: none"> Identify privacy related incidents. Monitor adherence to internal non-compliance and resolution procedures. Monitor adherence to customer privacy complaint and dispute resolution procedures. Monitor events (firewall, IPS, application, etc.) for privacy breaches daily. Review the privacy risk assessment.

The examples in this table were derived from [12] and [16]. ‘Administer Security Controls’. This process area contains the following practices:

- Establish responsibilities and accountability for security controls and communicate them to everyone in the organisation.
- Manage the configuration of system security controls.
- Manage security awareness, training, and education programs for all users and administrators.
- Manage periodic maintenance and administration of security services and control mechanisms.

CMMs also define capability levels, or maturity levels, for each process area. Capability or maturity levels are usually classified as ranging from zero (meaning there is no capability in this process area) to five (meaning this process area is well managed and that it has reached the stage where optimisation or continual improvement is all that is left to achieve). Five on this scale thus indicates a mature state.

We have used the definitions of capability maturity models from the [3] and [16] to define a privacy capability maturity model (PCMM) as: *a reference model of mature*

information privacy protection processes and associated practices used to improve and appraise an organisation’s capability to protect the information privacy of its data subjects. ‘Data subjects’ here refers to the people about whom the information relates.

To illustrate the PCMM we show three example process areas and some of the practices that may comprise these process areas in Table I. An examination of these example practices in the process areas in Table I reveals that the PCMM addresses the following: privacy policies (through developing and communicating such policies); people (by means of assigning responsibilities); processes (by establishing and monitoring procedures for non-compliance, as well as complaint and dispute resolution); technical privacy matters (by reviewing applications, infrastructure, systems, web-sites and by monitoring the associated events).

In Table II we show how the capability for these process areas would be appraised in a PCMM by utilising the generic privacy maturity (or capability) levels from [14].

TABLE II
GENERIC MATURITY LEVELS

Maturity Level	Description
0: Non-existent	No activities are performed.
1: Initial	Activities are ad hoc, with: <ul style="list-style-type: none"> No defined policies, rules, or procedures. Eventually lower-level activities, not coordinated. Redundancies and lack of teamwork and commitment.
2: Repeatable	The privacy policy is defined, with: <ul style="list-style-type: none"> Some senior management commitment. General awareness and commitment. Specific plans in high-risk areas.
3: Defined	The privacy policy and organization are in place, with: <ul style="list-style-type: none"> Risk assessments performed. Priorities established and resources allocated accordingly. Activities to coordinate and deploy effective privacy controls.
4: Managed	A consistently effective level of managing privacy, privacy requirements, and considerations is reflected in organization, with: <ul style="list-style-type: none"> Early consideration of privacy in systems and process development. Privacy integrated in functions and performance objectives. Monitoring on an organizational and functional level. Establishment of quantitative quality goals Periodic risk-based reviews.
5: Optimizing	Continual improvement of privacy policies, practices, and controls, with: <ul style="list-style-type: none"> Changes systematically scrutinized for privacy impact. Dedicated resources allocated to achieve privacy objectives. A high level of cross-functional integration and teamwork to meet privacy objectives. Measurement against quantitative quality goals

Slightly modified from [14].

The table also indicates the progression from each level of maturity to the next and what is required at each level. It is instructive to note how the table emphasises the importance placed on privacy policies: the crucial factor in the progression from level one to level three is the development and institution of a privacy policy. This highlights the fact that policies serve as the foundation of PCMMs.

B. Privacy Enhancing Technologies

In this section we define privacy enhancing technologies (PETs) and classify PETs for the purpose of our argument.

Because there is no single, authoritative definition of a privacy enhancing technology (PET) [21], we have chosen to adopt the definition by Burkert in [2] that defines PETs as “technical and organisational concepts that aim at protecting personal identity”. This definition allows us to differentiate between what we call *technical PETs* and *organisational PETs*.

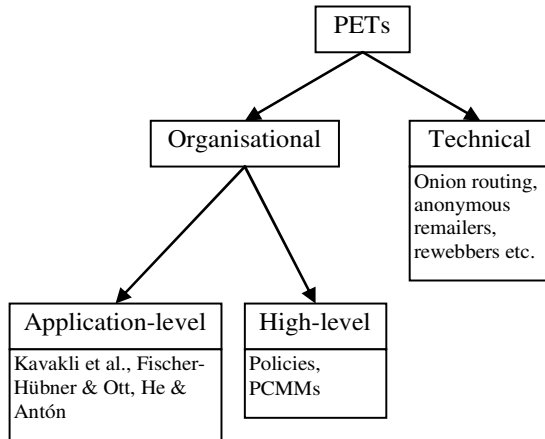


Fig. 1. Classification of PETs.

Technical PETs are designed to solve specific technical problems, mostly with regard to the maintenance of privacy on public networks such as the Internet. This is usually accomplished by using software [19] that ensures anonymity. The defining feature of these PETs is that they do not take organisational context into consideration [19]. The term privacy enhancing technologies is often used in the literature to refer to these technical PETs [27]. Onion routers, anonymous re-mailers and rewebbers [13] are all examples of technical PETs.

Organisational PETs, on the other hand, are designed to protect information privacy protection within an organisation. This is a much broader class of PETs as one may include organisational privacy policies and even disciplinary policies in this class. We place PCMMs in this class of PETs as PCMMs are organisational by definition. A number of other PETs in this class focus on facilitating appropriate access to information within an organisation. The appropriateness of access is usually a function of the organisation’s privacy policy and any applicable legal restrictions. If an organisation’s privacy policy states, for example, that staff in the marketing department may not have access to customers’ banking details, these PETs will prohibit them from gaining such access.

Organisational PETs usually utilise requirements engineering techniques, various access control methods, or some combination of both, to take organisational context into account. We call these PETs *application-level organisational PETs* (ALO PETs) because they are primarily designed to build access to and control of private information into an organisation’s information systems [10] [15] [19]. ALO PETs help mitigate the risk of private information on information systems being accessed by

inappropriate individuals. They also mitigate the risk of inappropriate flow of private information through an organisation’s information systems. Examples of application-level organisational PETs include:

- Kavakli et al.’s ‘PriS’ conceptual framework [19], which takes the privacy requirements and goals of a business into account when determining system requirements – it uses requirements engineering techniques.
- Fischer-Hübner and Ott’s implementation of an access control-based PET [10] that enforces privacy policies for data access and usage.
- He and Antón’s framework [15] which uses role engineering (a form of requirements engineering) to specify roles for a role-based access control approach to modelling privacy requirements within organisation’s applications.

Because of limitations on space, we do not elaborate on the ALO PETs presented in this paper.

We have not yet dealt with policies and PCMMs, which are also organisational PETs. We call such PETs *high-level organisational PETs* (HLO PETs) because they are usually implemented at a high level within an organisation.

III. TOWARDS A FULLY DEVELOPED PRIVACY CAPABILITY MATURITY MODEL

Our review of the literature revealed that there currently exists no fully developed capability maturity model (CMM) that deals specifically with privacy. The background detail we present on PCMMs in Section II helps address this issue by describing the essential elements of PCMMs. In this section we discuss the current state of CMMs and what is still needed before a PCMM can be fully developed.

The CMM developed at Carnegie Mellon University has served as the basis for the present security-specific capability maturity models. These include: the SSE-CMM [16], which is now ISO/IEC standard 21827; the United States National Security Agency’s INFOSEC Assurance Capability Maturity Model (IA-CMM) [17]; and the maturity model contained in the IT Governance Institute’s Control Objectives for Information and related Technology (COBIT) [6]. While these maturity models do take privacy into account, they do not treat it comprehensively enough to enable the adequate implementation of information privacy protection in an organisation (especially not in the case of telecommunication service providers). Generic privacy maturity levels are presented by Hahn et al. [14], however Hahn et al. present this for illustrative purposes and do not define the processes and practices required to fulfil our definition of a PCMM. In order to develop a PCMM fully, a complete enumeration of privacy-related processes together with a comprehensive set of associated privacy practices is required – in addition to the model presented in [14].

Our review of the literature furthermore revealed only one attempt to develop a comprehensive set of privacy practices – the Generally Accepted Privacy Principles (GAPP) [12] document drafted by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants.

While we believe that the practices contained in [12] are sufficient for the purposes of a PCMM, a complete and detailed description of privacy-related processes upon which these practices could be mapped is still necessary to complete the development of a PCMM. Our review of the literature has found no such complete and detailed description.

IV. AN ARGUMENT FOR USING PRIVACY CAPABILITY MATURITY MODELS IN THE TELECOMMUNICATIONS INDUSTRY

The main premise of our argument is that the protection of information privacy within large organisations such as telecommunication service providers is not simply a technical challenge: in order to take organisational context into account it is necessary to also consider policies, processes, and people.

In the discussion that follows we build our argument for the use of PCMMs by going into detail about why policies, processes and people are important in an organisation (we devote a section to each area). We show, by way of example, some of the risks associated with each area. We conclude our argument by discussing why PCMMs are well suited to dealing with these risks. We also discuss some of the disadvantages of PCMMs, and, in light of one disadvantage, we emphasize why PCMMs and ALO PETs provide an optimal solution to the problem of protecting organisational information privacy.

A. Policies

Privacy policies are the first and most important step in implementing an organisation-wide privacy protection regime. We have adapted Rees et al.'s definition of information security policies [23] to show how privacy policies serve as the basis for information privacy: *Privacy policies are generally high-level, technology neutral, concern risks, set directions and procedures, and define penalties and countermeasures if the policy is transgressed, and must not be confused with implementation-specific information, which would be part of the privacy standards, procedures, and guidelines. Privacy policies are created by empowered organisational representatives from human resources, legal and regulatory matters, information systems, public relations, security, privacy, and the various lines of business.* Privacy policies begin by creating an awareness of information privacy protection amongst senior management during their creation and approval. Awareness is important for the proper consideration of privacy in decisions such as new business ventures, partnerships and services. In the absence of the guidance provided by privacy policies, individuals tend to operate in a vacuum regarding decisions about private information [26]. This may result in an inconsistent approach to decision making in large organisations like telecommunications companies. Since well formulated policies are created with legal and regulatory input, the absence of guidance may result in decisions that contravene law, good governance and good business ethics. A decision, for example, to share customer data such as name, address, and banking details etc. with business partners in a new service offering without first

obtaining customer consent may have legal consequences damaging to the organisation. The penalties for contravention specified in privacy policies also deter individuals from accidentally or wilfully violating information privacy.

Another important advantage of privacy policies is that they enable the use of a large number of organisational PETs that are based on requirements engineering and access control methodologies because both types usually depend on the specifications and restrictions contained in privacy policies [1] [10] [15] [19].

B. Processes

Business processes predicated on privacy follow from privacy policies. When processes are well defined they provide the guidance that is needed at the operational level. For example, a well defined process that describes how customer transactional data should be released may reduce the risk of such data being released contrary to legal or regulatory requirements. *Customer transactional data* here refers to data about transactions performed using the services provided by the organisation (e.g. call records for telephone, SMS, and data calls, as well as the associated times, durations, bandwidth usage and location). In addition to this, impending legislation, such as the Privacy Bill, may necessitate new business processes or the re-engineering of existing ones. Principle seven of the Privacy Bill grants individuals the right to correct data held by an organisation, or, if an organisation is not willing to do so, the right to have “attached to the information a statement of the correction sought but not made” (this can be found in Annexure B of [9] at 22(1)(a) and 22(1)(b)). Telecommunications organisations will therefore need to have processes in place to make provision for customer requests and disputes about personal information.

C. People

Policies and processes are not effective if people are unaware of them. In order to adopt an organisation-wide stance towards information privacy protection, the relevant people need to be made aware of what information privacy is, why it is important to protect, and how to protect it while carrying out their particular function [11] [26]. Privacy is best built into systems at design-time [11]. Where engineers or developers fail to take privacy into account at design-time, costs may be incurred due to systems having to be ‘retro-fitted’ to accommodate privacy imperatives.

Another key advantage of making staff aware of privacy is that it reduces the likelihood of successful social engineering or ‘pretexting’ attacks, such as the attacks against AT&T reported in the press [28] in which data brokers fraudulently obtained the private data of AT&T customers using false pretences. In the United States these attacks have become so prevalent that a bill entitled ‘Consumer Telephone Records Protection Act’ has been proposed in Congress. This bill, if passed, will force telecommunication companies to contact customers if the customers’ records have been improperly accessed [8].

A compliance function within an organisation is important in ensuring that people adhere to privacy policies as research

has shown that practices can often vary from stated policies where sufficient attention is not given to compliance [26]. Compliance can often be made part of the responsibilities of an internal audit department where such a department exists in the organisation [14].

The ‘people’ aspect also extends to the provision of new organisational positions intended specifically for the adherence to privacy laws and regulations. The Privacy Bill requires an Information Protection Officer whose responsibilities include: encouraging compliance with the information protection principles in the Bill; dealing with requests made to the organisation pursuant to the Bill; working with the proposed Information Protection Commission in relation to any investigations of the organisation it may conduct; and otherwise ensuring compliance with the provisions of the Bill (this can be found in Annexure B of [9] at 46(1)(a)-(d)). Organisations in the European Union and the United States have already set a precedent in this regard by creating the Chief Privacy Officer role within organisations.

D. Discussion

We have argued above that it is vital to take policies, processes, and people into account when implementing information privacy protection across large organisations such as telecommunication service providers. We have also shown that each of these areas poses its own risk to information privacy. PCMMs distinguish themselves from other approaches to organisational informational privacy because they take policies, processes, people – as well as the technical aspects of information privacy – all into account in a comprehensive and integrated way. By doing this, they allow organisations to deal effectively with the risks posed by each of these areas.

In large organisations implementing information privacy protection can be a difficult task due to organisational complexity (e.g. many business units and multiple layers of management). Since PCMMs are intrinsically organisational they are particularly well suited to dealing with this complexity.

The maturity or capability levels in PCMMs also allow an organisation to gauge their progress in implementing information privacy. Implementation targets can be set to ensure accountability for those responsible for rolling out information privacy in the organisation and these can be used to ensure the implementation occurs correctly and on time.

We have concentrated on the virtues of PCMMs in this section, they are not without their drawbacks. A significant disadvantage of PCMMs is that they offer a top-down approach to implementing information privacy. We believe that while it is advantageous to set the proverbial ‘tone at the top’ by having top-level management buy-in for an implementation, any implementation that proceeds without it is not likely to succeed. Thus, PCMMs are reliant on top-level management buy-in order to be effective.

Another disadvantage of PCMMs is that they do not, on their own, enforce an organisation’s privacy policies at the application-level. In other words, they do not ensure that the private information in an organisation’s information systems

is treated in accordance with the organisation’s policies. This is precisely the risk ALO PETs were designed to mitigate.

We therefore suggest that the optimum approach to implementing information privacy protection in an organisation is a combination of a PCMM and ALO PETs. We believe the two can, and should, exist symbiotically for the following reason: PCMMs would help to determine where and how to use ALO PETs, which would in turn help mitigate the application-level risk not addressed by PCMMs.

V. CONCLUSION

We have shown in this paper why PCMMs are useful in protecting the information privacy of customers of telecommunication service providers and other large organisations that hold considerable amounts of personal data. We have shown why we believe that it is necessary for PCMMs to be used in conjunction with ALO PETs to achieve an optimal level of information privacy. We also performed a classification of PETs to support our argument (specifically, to derive the term ALO PETs). Additionally, we have shown the essential elements of PCMMs since there are no fully developed PCMMs in the literature.

Much research still needs to be undertaken before PCMMs are fully developed. The process areas involved in implementing and maintaining information privacy have yet, for example, to be determined. We believe this is because privacy protection is not as mature a discipline as information security. The lessons learned from implementing organisational information security have yet to be learned in implementing information privacy because far fewer organisations have to date attempted the latter. Completion of this research is likely to take years rather than months.

Subsequent to (or concurrent with) determining process areas, there is also a need for research on integrating security and privacy standards (including CMMs) [25] so as to ensure the feasibility of privacy standards. This is necessary since information security departments are likely to be dealing with information privacy [22]. Because there is a close relationship between privacy and security, the integration of these functions will reduce redundancy and the cost of implementing information privacy.

ACKNOWLEDGMENT

The authors thank Rudi Opperman at MTN Group Management Services and Itumeleng Moerane at Vodacom Government Relations and Regulatory Affairs for their time and assistance.

This material is based upon work supported by the National Research Foundation under grant number 2054024. Any opinion, findings, conclusions or recommendations expressed in this material are those of the authors and the NRF does not accept any liability thereto.

REFERENCES

- [1] M. Backes, W. Bagga, G. Karjoth, and M. Schunter, “Efficient Comparison of Enterprise Privacy Policies”,

- in *Proc. 2004 ACM symposium on Applied computing*, Nicosia, Cyprus, 2004.
- [2] H. Burkert, "Privacy-enhancing technologies: typology, critique, vision", in *Technology and Privacy: The New Landscape*, 1st ed, P. E. Agre and M. Rotenberg, Eds. Massachusetts: The MIT Press, 1998, pp. 125-142.
- [3] *Capability Maturity Model Integration (CMMI) Version 1.1 Overview*, Carnegie Mellon Software Engineering Institute, Pittsburgh, PA, 2005. Available: <http://www.sei.cmu.edu/cmmi/adoption/pdf/cmmi-overview05.pdf>
- [4] R. Clarke, "Information Technology and Dataveillance", *Communications of the ACM*, vol. 31, no. 5, pp. 498-512, 1998.
- [5] R. Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", Department of Computer Science, Australian National University, 2006. Available: <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html>.
- [6] *COBIT 4.0*, IT Governance Institute, Rolling Meadows, Illinois, 2005. Available: http://www.itgi.org/template_ITGL.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=27263
- [7] *The Constitution of the Republic of South Africa*, Chapter 2, Section 14, South Africa, 1996.
- [8] Consumer Telephone Records Protection Act of 2006, Bill no. S.2178, The Library of Congress, Washington DC, 2006. Available: <http://thomas.loc.gov/cgi-bin/query/z?c109:S.2178>:
- [9] *Discussion Paper 109, Project 124, Privacy and Data Protection*, South African Law Reform Commission, Pretoria, 2005.
- [10] S. Fischer-Hübner, and A. Ott, "From a formal privacy model to its implementation", in *Proc. 21st National Information Systems Security Conference*, Arlington, VA, 1998.
- [11] S. Fischer-Hübner, and H. Lindskog, "Teaching Privacy-Enhancing Technologies", in *Proc. IFIP WG 11.8 2nd World Conference on Information Security Education*, Perth, Australia, 2001.
- [12] *Generally Accepted Privacy Principles – A Global Privacy Framework, CPA/CA Practitioner Version*, American Institute of Certified Public Accountants & Canadian Institute of Chartered Accountants, Toronto, Canada, 2006. Available: http://www.cica.ca/index.cfm/ci_id/258/la_id/1.htm
- [13] D. A. Gritzalis, "Embedding privacy in IT applications development", *Information Management & Computer Security*, Vol. 12, No. 1, pp. 8-21, 2004.
- [14] U. Hahn, K. Askelson, and R. Stiles, *Global Technology Audit Guide 5: Managing and Auditing Privacy Risks*, Institute of Internal Auditors Research Foundation, Altamonte Springs, Florida, 2006.
- [15] Q. He and A. I. Antón, "Framework for Modeling Privacy Requirements in Role Engineering", in *Proc. 9th International Workshop on Requirements Engineering: Foundation for Software Quality*, Klagenfurt/Velden, Austria, 2003.
- [16] *Information technology – Systems Security Engineering – Capability Maturity Model (SSE-CMM©)*, ISO/IEC Standard 21827, 2002.
- [17] *INFOSEC Assurance Capability Maturity Model (IA-CMM)*, National Security Agency, Fort Meade, Maryland, 2004. Available: <http://www.iatrp.com/iacmm.cfm>.
- [18] Jordaan, Y. 2003, "South African Consumers' Information Privacy Concerns: An Investigation in a Commercial Environment", PhD Thesis, University of Pretoria, Pretoria.
- [19] E. Kavakli, C. Kalloniatis, P. Loucopoulos, and S. Gritzali, "Incorporating privacy requirements into the system design process: The PriS conceptual framework", *Internet Research*, vol. 16, no. 2, pp. 140-158, 2006.
- [20] S. Lau, "Good Privacy Practices and Good Corporate Governance – Hong Kong Experience", in *Proc 23rd International Conference of Data Protection Commissioners*, Paris, France, 2001. Available: http://www.cnil.fr/conference2001/eng/contribution/lau_contrib.pdf.
- [21] *Privacy Enhancing Technologies*, META Group Report to the Danish Ministry of Science, Technology and Innovation, 2005. Available: <http://www.itst.dk/image.asp?page=image&objno=198999309>
- [22] *Protecting the digital assets – The 2006 Technology, Media & Telecommunications Security Survey*, Deloitte Touche Tohmatsu, 2006. Available: <http://www.deloitte.com/dtt/research/0,1015,cid%253D137260,00.html>
- [23] J. Rees, S. Bandyopadhyay, E. H. Spafford, "PFIREs: a policy framework for information security", *Communications of the ACM*, vol. 46, no. 7, pp. 101-106, 2003.
- [24] *Regulation of Interception of Communications and Provision of Communication-related Information Act*, South Africa, 2002.
- [25] J. Robbins and J. T. Sabo, "Managing information privacy: developing a context for security and privacy standards convergence", *IEEE Security & Privacy*, vol. 4, no. 4, pp. 92-95, 2006.
- [26] J. H. Smith, "Privacy policies and practices: Inside the organizational maze", *Communications of the ACM*, vol. 36, no. 12, pp. 105-122, 1993.
- [27] H. T. Tavani and J. H. Moor, "Privacy protection, control of information, and privacy-enhancing technologies", *ACM SIGCAS Computers and Society*, vol. 31, no.1, pp. 6-11, 2001.
- [28] E. White, "AT&T file suit to follow fraudsters' trail", *Independent Online Technology*, 2006. Available: http://www.ioltechnology.co.za/article_page.php?iArticleId=3407233.

Kamil Reddy is a PhD student with the Information and Computer Security Architectures research group at the University of Pretoria's Department of Computer Science. He holds an MSc in Computer Science from the University of Natal Durban (now University of KwaZulu-Natal) and is a member of the IEEE and ACM.

H.S. Venter is a Senior Lecturer with the Information and Computer Security Architectures research group at the University of Pretoria's Department of Computer Science. He holds a PhD in Computer Science from Rand Afrikaans University (now University of Johannesburg). He is a member of IFIP WG 11.9 (Digital Forensics), SAICSIT, and ISSA.