An Environmentally Adaptive Conceptual Framework for Addressing Information Privacy Issues in Digital Ecosystems

Geoff D. Skinner and Elizabeth Chang

Centre for Extended Enterprises and Business Intelligence, Curtin University of Technology, Perth, WA, AUSTRALIA
e-mail : Geoff.Skinner@newcastle.edu.au, Elizabeth.Chang@cbs.curtin.edu.au

***Abstract*—The evolution of Collaborative Environments towards Digital Ecosystems comes with increased risks to personal data and entity privacy. To address privacy protection concerns we propose a conceptual framework that integrates technical, legal and contextual components to provide comprehensive system wide privacy. Part of the framework is a Privacy Evaluator Module (PEM). The PEM's function is to assimilate individual information system privacy protection strategies into a consistent ecosystem wide approach.**

***Index Terms*—Privacy, PETs, Privacy Regulations, TLC Privacy Protection, Privacy Evaluator Module.**

I. Introduction

The field of Digital Ecosystems' (DE) was first defined in 2002 [1] and provides many innovative ways of applying information and communications technology. Recent research into the field of Digital Ecosystems has produced a number of potentially beneficial results for knowledge sharing and increasing productivity for small to medium enterprises. DE's by their very nature promote cooperation and the development of open and adaptive technologies [2]. Such environments present many interesting issues and challenges for information privacy and data security. As with classical computer system evolution the relatively new field of digital ecosystems is already at risk of following a similar path of overlooking information privacy concerns. Clarke [3] defines information privacy as being a combination of communications privacy and data privacy. He formally defines it as '... the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves' [3]. An individual's concern about their information privacy is a significant issue regardless of the technology used to implement the information systems the entities are interacting with. It is widely regarded that many of the current information systems privacy inadequacies derive from the fact that privacy was never a serious consideration during the development life cycle of the systems [4]. This is in addition to the fact that the idea of privacy is itself very subjective in nature, unique to each individual and influenced by a broad range of factors from context to culture [5, 6]. From a financial perspective the ability to place monetary values on individual privacy is very difficult and therefore hard to integrate such factors into system design specifications and costing [7].

Modern privacy solutions are often derived from the application, both in combination and isolation, of the four main models of privacy protection [8]. The models are Comprehensive Laws, Sectoral Laws, Self Regulation, and Technologies of Privacy. Of interest to our own work is the impact of digital ecosystems on information privacy and what modifications are required for privacy enhancing technologies (PETs) to operate effectively in digital ecosystems. The reason being is that many of the technology of privacy solutions rely on varying levels of computationally secure methods, such as encryption, to provide security and privacy of personal data [9]. With progression to more open collaborations and increased data sharing, application and regulation of personal data protection methods will become more complex. Privacy considerations in Digital Ecosystems have to date only received minimal attention. Mention has been made of privacy from a civil liberties perspective [10]. In this context privacy protection is seen as being offered through legal and regulatory methods. Privacy has also been identified as one element of the 'Top Ten Truths About Digital Ecosystems' [11]. Privacy protection enforcement and information security issues arise due to the self-organizing and dynamic nature of digital ecosystems.

The focus of this paper is to provide a foundational perspective of our work investigating Information Privacy issues in the realm of digital ecosystems. We propose that solutions to address the increased privacy threats posed by digital ecosystems are fundamentally similar to those required for current information privacy issues for collaborative environments. That is, not only does Information Privacy conformance need to be integrated from system inception, but an effective privacy solution must be a symbiotic moulding of technical, legal, and social elements. Due to the complex systems involved and their self-organizing nature no single model of privacy protection is adequate for digital ecosystems. Rather, all models need to be incorporated into the environments and continually monitored and updated to ensure they maintain privacy while also facilitating the functionality of digital ecosystems.

The rest of the paper follows a common structure outline as follows. Section 2 provides relevant background material on Information Privacy for data at rest and in transit. Additionally, what constitutes a Digital Ecosystems and how they have evolved is also discussed. Current collaborative environment approaches to Information Privacy and Data Security is included in Section 3. Section 4 provides our proposals on what can be done to insure information privacy protection in Digital Ecosystems. The TLC Framework for Digital Ecosystems is detailed in Section 5. A brief conclusion and future work is provided in Section 6.

1-4244-0470-3/07/$20.00 ©2007 IEEE

II. Background and Related Work

Digital Ecosystems and the operational environment they foster may inherent many of the same privacy issues that are faced by classical information systems and communication technologies [12]. However, it is the possibility that many unforeseeable privacy problems may be part of the new technology and therefore need investigation in the digital ecosystem context. Our focus is on Information Privacy rather than Information Security, and specifically the development of a comprehensive system wide approach to information privacy. From a technological perspective this involves the development and integration of Privacy Enhancing Technologies [13] into Digital Ecosystems. The uniqueness of privacy in terms of its subjective nature and openness to individual interpretation and representation has allowed it to evolve with advances in technology, society, culture and values [14]. In the field of IS research privacy solutions are not always based on technological approaches. The use and enforcement of legal regulations, laws (sectoral and comprehensive), and even self regulation attempts will still be applicable and perhaps even more significant to information privacy in digital ecosystems. However, protection against intentional malicious attacks is still heavily reliant on technological solutions. Therefore, when approaching information privacy issues in the environments that encourage openness, information sharing and dynamic configurations all models of privacy protection should be evaluated and utilized where ever possible.

According to the Common Criteria [15] privacy requirements for identity and privacy protection are concerned with anonymity, pseudonymity, unlinkability and unobservability. These set of requirements also provide a baseline level of protection requirements for privacy enhancing technologies (PETs). A major set of tools that facilitate these requirements is that of encryption. Encryption in general is used to protect information stored on a computer or transmitted over communication networks. By preventing access to data it also helps protect privacy. A number of PETs make extensive use of encryption in some manner to help protect privacy. These include the Identity Protector [16], Privacy Shield [17], and Privacy Protector [18]. The form of encryption used is normally based on some form of Public Key Infrastructure (PKI), RSA, and other computationally hard (from a classical sense) algorithms. With such requirements comes the need for some consistent key storage medium as well as a way of ensuring the keys are correct and enforceable. This is a challenging issue then for environments that are able to dynamically configure themselves and allow an equally diverse set of system users. Digital ecosystems are about building virtual communities sharing business, knowledge, and infrastructures [19]. Operation of such environments also allows the connection of multiple data sources. When used in combination with advanced data mining and profiling algorithms, access to and generation of, personal profiles would be more readily available community members. This is a major risk to users wishing to protect their privacy and avoid being subject to profiling and other targeted personal data analysis.

With any new information technology with potential risks for privacy also come the potential for privacy benefits. The field of digital ecosystems is no exception. Perhaps the biggest advantage of the new technology is the fact it is so new. Being in its infancy allows system designers to hopefully learn from previous mistakes, in particular the design oversights of classical systems when considering information privacy. Privacy by design is a key concept that should be applied to all new information systems, whether they are classical or dynamic in nature. Even hybrid combinations of both technologies should offer better privacy protection to the users of the systems. For example, while all aspects envisaged for digital ecosystems are still some time away from general use, there has been substantial research conducted on privacy in collaborative environments and e-Business infrastructures [17, 20].

Collaborative environments and networked organizations may not support all the traits expected from digital ecosystems. However, they are part of the evolutionary path that has led to digital ecosystems [1], so many of their privacy issues that have been and are currently being investigated are also applicable. What is important is the fact that information privacy benefits from any type of exposure. Raising user and system owner's awareness is an important phase in the over all process of protection of personal data and entity privacy. Digital ecosystems are aimed at empowering small to medium enterprises allowing them to form transitory structures through collaboration. Digital ecosystems not only facilitate knowledge transfer but also resource and expertise sharing. An ideal situation is to ensure that privacy best practises can be formulated and spread by the sharing of resources. Perhaps one member of the community does provide privacy protection to which other members are able to benchmark against. The synergy of sharing community resources should not be limited to only business related objectives. Rather it should also encompass the knowledge of providing effective information privacy and security. Our work serves two purposes then. Firstly to highlight potential threats to information privacy and any advantages that may be gained from digital ecosystems. Secondly, we propose a framework to address the threats to privacy in digital ecosystems. We show that many of these solutions will require a unique moulding of technical, legal and social elements to ensure information privacy is preserved.

III. Information Privacy in Information Systems

The evolutionary path to digital ecosystems is one that is composed of a number of phases. Each phase is part of a continuous process made up of a set of sequential steps [1]. These steps represent the progressive adoption of more complex information systems and increasing interconnection between them. The phases are listed as being: E-mail; Web-presence; E-Commerce; E-Business; Networked organizations; and Digital Ecosystems. In each phase the level of interaction and data exchanges between different entities is increasing. That is, more information is required at each progression through the sequential steps in order for the phase to function correctly. For example,

email may take place between any two entities. The content of the emails, option of replying and who they are sent to and received by is under the control of the entities involved. The main risk to privacy at this level of interaction is email interception, viewing by unknown entities, and unauthorized access. Towards the later phases of the evolution such as Networked organizations, many entities, systems and processes are involved. The amount of data exchanged between member organizations has increased significantly and so to has the risk to entity privacy. In our research context an entity can be an individual, a group, or an organization. A formal Information Privacy taxonomy is provided in [21] where these terms are defined in more detail and applied to our own work.

Digital ecosystems are the next evolutionary step in the move towards interaction across multiple domains of multi-disciplinary nature. Current collaborative environments are viewed as being to rigorously defined, not transparent enough, and not flexible enough to foster dynamic collaboration between small to medium enterprises. However, central to digital ecosystems infrastructure is collaborative environments composed of any number of information systems. Therefore, privacy issues found in collaborations are also applicable to digital ecosystems. Further, the digital species of digital ecosystems, consisting of software, databases, applications and services, are components of information systems all requiring privacy protection. Collaborative environments provide a data and knowledge sharing service. Whether they are client-server, P2P, grid and web services or digital ecosystems models they support information communication that enables shared understanding of concepts. When ever personal data or private information is involved in this service it can have both a positive and negative impact on privacy. When the knowledge sharing is about how to protect privacy then this is a privacy benefit. When the knowledge sharing involves unauthorized or unknown disclosure of personal data then this is a privacy risk. Therefore we endorse the protection of privacy at all levels or within all digital species of digital ecosystems. That is, privacy protection should form an integral part of all information systems within the digital ecosystem with consistent privacy principles and practices enforced throughout the digital ecosystems life cycle.

As mentioned in the introduction four common models of privacy protection [8] are: Comprehensive Laws; Sectoral Laws; Self Regulation; and Technologies of Privacy. Our earlier work [17] has shown that the use of a single model is ineffective for providing privacy protection. To achieve a comprehensive privacy solution a combination of the models is required. Which models to use together is determined by the operational conditions of the environment. For example, in those regions where there is a lack of comprehensive laws then increased application of self regulation methods and increased use of PET's (Privacy Enhancing Technologies) would be required. The models are limited in that they only represent clearly defined ways of providing protection. They are often unable to represent individual preferences and the influences of changing situations and different contexts. We propose that in order to achieve privacy protection suitable for all entities, especially for environments as dynamic as digital ecosystems, then a framework is required that is capable of performing the following functions:

- Integrates all four models of privacy protection and allows them to be modified as required
- Allows privacy preferences and protection to be modified for different situations
- Allows privacy preferences and protection to be adaptable to different contexts
- Ensures that privacy 'best practise' is enforced across the whole ecosystem

The last point refers to taking a restrictive approach to privacy rather than an unrestrictive approach. That is, where a number of information systems are collaborating at any given time, then the most comprehensive and restrictive data protection and privacy operational principles from the member systems should be applied and enforced across the whole ecosystem. This function is against key objectives of digital ecosystems, that being openness, transparency and information sharing. However, in many countries and regions privacy protection is the law and must be upheld. This approach also follows the privacy design method of 'opt-in' rather than 'opt-out'. All transactions should be privacy sensitive by default rather than requiring the data providing entity to ensure their personal data is protected. Privacy protection is the responsibility of system owners and not system users.

IV. THE TLC APPROACH TO INFORMATION PRIVACY

Research to date strongly indicates that no single model of privacy protection is sufficient to provide a complete information privacy solution [8]. Therefore, we propose that a solution to this issue is to develop systems and operating environments that integrate a symbiotic moulding of all four models of privacy protection. In addition, privacy by design and information system Hippocratic principles [4, 22] should be adhered to throughout the systems life cycle. To compliment the for-mentioned factors and provide robust information privacy protection architectures, the operating contexts [23, 24] as well as social and cultural environmental conditions need to be accounted for within the framework during development, deployment and operation.

Technology achievements advance at a rapid rate bringing new threats to privacy and an entities identity. Many PET's that have been proposed only deal with immediate threats to information privacy and do not look far beyond the current computational capabilities of systems and desired information sharing environments. Not only are the computational abilities of systems increasing but also their level of ubiquity. Pervasive computing environments are becoming more common, and when coupled with increased computational capabilities dramatically increase the risks to information privacy. So when these factors are considered ain conjunction with the increasing use of digital ecosystems there is a greater risk to entity privacy. Even early deployment of digital ecosystems that have not devoted time and effort to a complete information privacy evaluation,

impact assessment, and methodical approach to protection pose a serious threat to privacy. Many of the digital ecosystems currently in operation are still in their infancy and therefore it is very difficult to determine their actual impact on privacy. However, any system that promotes and supports the sharing of knowledge and resources must factor in privacy considerations.

Any sustainable privacy solution must make every effort to take into consideration all current and foreseeable future factors that pose a threat to information privacy. Therefore, we propose a framework entitled T.L.C. (Technical, Legal, and Contextual) Privacy Protection, referred to as TLC-PP. It is an approach that combines all four models of privacy protection [8], as well as consideration for the influence of social and cultural ideals and perceptions. It supports the implementation and methods of enforcement for both comprehensive and sectoral laws, self regulation and certification schemes, and the impact the operating context has on all of these components [23, 24]. The TLC-PP objective is to address the issue of information privacy that is at risk from the increasing computational capacities, distributed nature, and information sharing objectives of current and future computing environments. In particular, we are concerned with the possibility that in the near future, with the evolution of digital ecosystems, computing environments will have very dynamic and hard to defined operating boundaries. The diagram in Figure 1 provides a visual representation of the three TLC cornerstones of privacy protection and their respective components.

Technological advances should be applied in equal measure to ensure privacy protection. With increased collection and processing of information it is imperative that industries and researchers contributing to technological advances also develop complimentary methods of privacy protection. For example, with the advent of Digital Ecosystems there is the risk of compromising many of the widely used privacy technologies that help provide privacy protection. In order to offset this problem then it must be possible to leverage the new technology to also provide better awareness of risks to privacy. With awareness comes increased concern and research interest and like our own framework may promote further solutions. Many of the current approaches to privacy protection can be extended for digital ecosystem use. This includes the design and operating objective of when ever possible the use of anonymous and pseudo-anonymous identities should be implemented. This approach to identity and privacy protection when taken at a conceptual level, abstracted from the technological implementation details, is applicable to all systems providing privacy. Therefore, no matter the computational capabilities, dynamic and distributed nature of the computing environment, PET's should provide anonymous and pseudo-anonymous services, use of anonymous transmission for data communications, and private information retrieval.

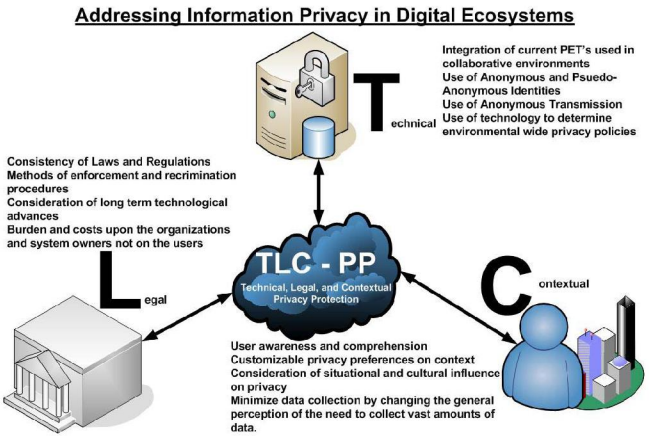

Fig.1 TLC-PP

Legal approaches to privacy protection have the advantage of being even further abstracted from technological advances. However, the need in the future will be to ensure consistency of privacy laws and regulations across all regions and countries. Equally important will be the ability to enforce the laws and regulations that are put in place. The burden and costs involved to pursue information privacy breaches should not be placed upon the user. Rather the onus should be on the system owners to ensure they correctly adhere to the privacy laws and regulations governing their operation. Currently the EU seems to be focusing on comprehensive privacy legislation rather than the sectoral approach seen in other countries and regions. Australia has made a number of promising steps towards improving their information privacy laws; however there still seems to be a lack of consumer awareness and organizational uptake. While this may be seen as a negative for current information privacy advocates at least one positive can be to be drawn from such a state. That is, it provides opportunities to incorporate measures that take into consideration future threats to information privacy such as the information sharing and dynamic nature of digital ecosystems.

Contextual conditions also play an important part in information privacy protection. Foremost of these initiatives should be increasing social awareness of data collection and usage. This is in combination with system users comprehending the need to protect their privacy and personal information from abuse. Not all users, groups, organizations and even societies and cultures perceive privacy the same. Further, certain situations and different contexts affect an entities need for and perception of privacy. Therefore, future systems need to allow users to customize their privacy preferences based on different contexts, social and situational conditions [23]. These environmental influences are what we have termed Contextual conditions for managing privacy. Entities and system users should also be able to clearly understand and comprehend the privacy and data usage policies of the system they are using. The key components then for Contextual privacy protection are adaptability to different contexts, changing situations, and individual perceptions and preferences.

V. TLC-PP Framework for Digital Ecosystems

Digital ecosystems are often viewed as holistic approaches to enterprise integration [25]. By definition they often seem to be in conflict with the ideas of privacy and data protection. DE's promote open resource sharing and knowledge access to all entity members with access being relatively easy to obtain. In order to ensure privacy is maintained throughout the symbiotic relationships, information privacy protection must be a fundamental component of the supporting infrastructure. The first step towards this goal is to try and model privacy protection on the environment it is to be integrated with. We propose that privacy should follow the analogy used throughout the digital ecosystem methodologies. That is, like natural biological ecosystems, the privacy protection species should be adaptable to local conditions. For example, as mentioned in Section 3 not all privacy laws are consistent across countries and regions. Therefore privacy protection in digital ecosystems than span multiple regions and borders would be different for each information system forming the infrastructure of the ecosystem. This becomes a serious issue when members of the collaboration may not be governed by any privacy laws or regulations. Therefore the overall objective for the TLC-PP framework is to take a restrictive approach to privacy, with the burden for privacy management placed on system owners and digital ecosystem members rather than system users.

The TLC-PP framework we are proposing is still at a conceptual level. We acknowledge that before a fully functional model can be realised advances in all areas are required. This will involve such initiatives as:

- A global baseline of privacy laws regulations governing personal data management and entity privacy.
- Further advances in technologies of privacy and their widespread adoption.
- Increased awareness of privacy and personal data management. System owners taking responsibility and everyone recognizing the individuality of privacy that is influenced by context and situation.

We also acknowledge that many digital ecosystems are being created from existing information systems that may not provide privacy protection. However, part of the framework integration is to evaluate current infrastructure and identify privacy issues that need addressing. As mentioned, the approach to privacy protection should be one that is able to adapt to local conditions and dynamic formation. With these limitations realised the remainder of this section explains the conceptual framework of TLC-PP for digital ecosystems.

Contextual components are often the most easily identified but the hardest to evaluate and implement. When we state that increased entity awareness of privacy protection is required there seems no clear method for achieving this. Therefore the best place is at system inception with system designers. If information systems are currently in operation then as part of their merging evolution into an ecosystem then part of the process should be integration of privacy protection. Membership to the ecosystem should also be mandated with entity privacy agreements. This may be digital signing or confirmation of privacy awareness statements as well as mandatory viewing of information system privacy policies. The use of privacy preferences should be made available to users that also incorporate situational and contextual elements [23].

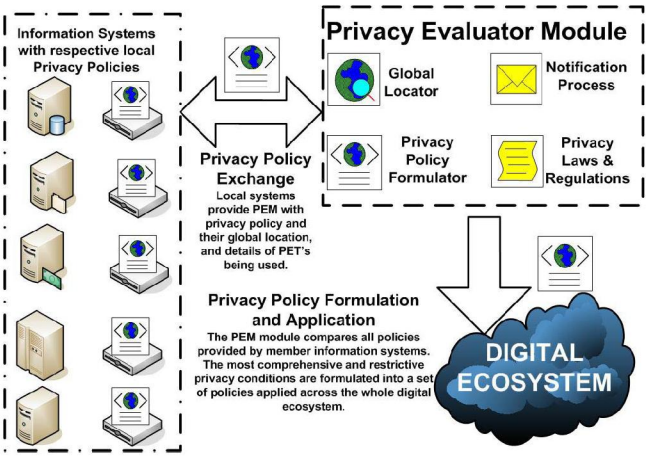

Fig.2 TLC-PP Framework with PEM Module

The critical component of the framework however is the Privacy Evaluator Module (PEM). This is an application module tasked with privacy management within digital ecosystems. Its main function is to ensure that by default the most comprehensive and restrictive privacy practices are maintained consistently across the whole digital ecosystem. The PEM will require each information system to determine and provide its operational origin. That is, state which region or country the system is located in and the privacy laws and regulations it is governed by. The PEM will be required to read the privacy policies of each system, provided in a P3P format [26], and determine the most restrictive conditions to govern all systems operating as part of the digital ecosystem. Notification will be provided to member system owners of the associated regions and countries the collaboration is operating across. Owners will be made aware of the possibility of specific privacy laws and regulations of those members. The actual details of the laws and regulations will not be provided by PEM, but rather the onus is on the system owners to ensure their privacy management practices comply. System owners may then be required to modify their local system privacy preferences to ensure they are compatible with the 'best practice' of the digital ecosystem. The additional benefit provided by membership in the ecosystem is access to privacy protection best practises and ensuring local systems meet the standard. Enforcement of the preferences and data protection will be provided by the continual upgrading and integration of the latest Privacy Enhancing Technologies. For example, a standard requirement should be the support of anonymous and pseudo-anonymous entity identities. Further all storage and transit of personal data should be done through encrypted means. A model of the PEM module and the operational TLC-PP framework is provided in figure 2. It is planned to extend the module to maintain updateable privacy laws and regulations for systems wide reference.

VI. Conclusion and Future Work

With any new technology there is a much to learn often through trial an error. Previous privacy mistakes and issues

that have been made with classical computing systems are ones that can be avoided or at least addressed with the evolution of digital ecosystems. Privacy laws, regulations and policies are applicable to any information systems, regardless of the operating environment. The issue is to ensure consistency and enforceability in environments that are dynamic and distributed. Our work is focused on the challenges faced to Information Privacy with the advent of digital ecosystems. We have proposed a symbiotic moulding of various privacy protection models into an approach we have termed TLC-PP (Technical, Legal, and Contextual Privacy Protection). The TLC-PP framework positions information privacy as a key objective of system design and operation. TLC-PP recognizes privacy risks of the dynamic nature of future digital ecosystems. Our ongoing work encompasses the continual integration and implementation of all models of privacy protection into the framework. An important objective of the research is to highlight the need for Information Privacy awareness from an early development stage. This can be further achieved by the integration of privacy by design principles and developing solutions that are dynamic and distributed to work cohesively with the operating conditions of digital ecosystems.

VII. REFERENCES

[1] European Commission, "Towards A Network Of Digital Business Ecosystems Fostering The Local Development", Discussion Paper, Septemeber, 2002.

[2] European Commission, "Technologies for Digital Ecosystems", http://www.digital-ecosystems.org

[3] R. Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html, September, 1999.

[4] G. Skinner and E. Chang, "PP-SDLC The Privacy Protecting Systems Development Life Cycle", IPSI-2005 FRANCE, April 23 till April 26, 2005.

[5] Y. (Sheila) He, D. N. Jutla, "Contextual e-Negotiation for the Handling of Private Data in e-Commerce on a Semantic Web," HICSS, p. 62a, Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06) Track 3 (2006).

[6] R. Wishart, K. Henricksen, and J. Indulska, "An access control scheme for ubiquitous computing environments based on context-dependent privacy preferences", ACISP 2005, The 10th Australasian Conference on Information Security and Privacy, Brisbane Australia, 4-6 July, 2005.

[7] S. Faja, "Privacy in E-Commerce: Understanding User Trade-Offs", Issues in Information Systems, Volume VI, No. 2, 2005.

[8] EPIC, "Privacy and Human Rights 2003", Electronic Privacy Information Centre, http://www.epic.org

[9] G. Skinner, S. Han, and E. Chang, "The Computational View of Information Privacy for Privacy Enhancing Technologies", The First International Conference on Legal, Security and Privacy Issues in IT (LSPI), 2006.

[10] J. Moore and J. Palfrey, "ICT and Entrepreneurship: Digital Business Ecosystems and the Law", Berkman Centre for Internet and Society, Harvard Law School..

[11] G. Moore, "Top Ten Truths About The Digital Ecosystem", Dealing With Darwin, June, 2006.

[12] IBM Research Report, "Views of Privacy: Business Drivers, Strategy, and Directions", IBM Research Division, Sept., 2003.

[13] I. Goldberg, "Privacy-enhancing technologies for the Internet II: Five years later", PET 2002, San Francisco, 2002.

[14] R.M. Davison, R. Clarke, J. Smith, D. Langford, and B. Kuo, "Information Privacy in a Globally Networked Society: Implications for IS Research", Communications of the Association for Information Systems, Volume 12, 2003, 341-365.

[15] Common Criteria Project, "The Common Criteria", http://www.commoncriteriaportal.org/.

[16] G.W. van Blarkom, J.J. Borking, and J.G.E. Olk, "Handbook of Privacy and Privacy-Enhancing Technologies", Privacy Incorporated Software Agent (PISA) Consortium, The Hague, 2003.

[17] G. Skinner and E. Chang, "A Conceptual Framework for Information Privacy and Security in Collaborative Environments", International Journal of Computer Science and Network Security, Vol. 6 No. 2B, Feburary 28, 2006.

[18] D.A. Gritzalis, "Embedding privacy in IT applications development" Information Management and Computer Security, Vol. 12 No. 1, 2004.

[19] F. Nachira, "What is a Digital Ecosystems?", Essence of a Digital Ecosystem, online paper, http://www.digital-ecosystems.org

[20] A. Ghosh, "Security and Privacy for E-Business", John Wiley and Sons, 2001.

[21] G. Skinner, S. Han, and E. Chang, "An Information Privacy Taxonomy", Emerald International Journal of Information Management and Computer Security, Volume 14 Number 4 2006.

[22] R. Agrawal, J. Kiernan, R. Srikant, Y. Xu, "Hippocratic Databases", 28th Int'l Conf. on Very Large Databases (VLDB), Hong Kong, 2002.

[23] G. Skinner and E. Chang, "Fair Privacy Principles and Preferences (F3P) – Evaluating Context Based Privacy Preferences", The 10th WSEAS International Conference on Computers, ICCOMP-06, Vouliagmeni, Athens, Greece, July 13-15, 2006.

[24] M. Ackerman, T. Darrell and D.J. Weitzner, "Privacy In Context", Massachusetts Institute of Technology Discussion Paper, http://www.eecs.umich.edu/~ackerm/pub/01a12/context-privacy.final.pdf.

[25] Syntel, "Building Your Own Digital Ecosystem: a Holistic Approach to Enterprise Integration", A White Paper Series, MI, USA.

[26] W3C, "Platform for Privacy Preferences (P3P)", Platform for Privacy Preferences Project, http://www.w3.org/P3