A Privacy Augmented Collaborative Environment (PACE)

GEOFF SKINNER
Faculty of Science and Information Technology
University of Newcastle
University Drive, Callaghan, NSW, 2308
AUSTRALIA

Abstract: - In order to sustain privacy in digital collaborative environments a comprehensive multidimensional privacy protecting framework is required. Such information privacy solutions for collaborations must incorporate environmental factors and influences in order to provide a holistic information privacy solution. Our Technical, Legal, and Community Privacy Protecting (TLC-PP) framework addresses the problems associated with the multi-facetted notion of privacy. The three key components of the TLC-PP framework are merged together to provide complete solutions for collaborative environment stakeholders and users alike. The application of the TLC-PP framework provides a significant contribution to the delivery of a Privacy Augmented Collaborative Environment (PACE).

Key-Words: - Information Privacy, Privacy Evaluator Module (PEM), Manual Privacy Management (MPM), Community Observed Privacy (COP), TLC-PP

1 Introduction

Collaborative environments fulfill a very important role in a knowledge society, providing a digital 'place' for the exchange of ideas and knowledge, seen as one of the most important activities of man [1]. The storing of data in a commonly accessible structure has both a great potential for the knowledge society as well as a high risk for the user's privacy. Here in lies one of the greatest challenges for collaborative environments. That is, a continual balance must be sought between the interests of open easily accessible information with the protection of personal data and entity privacy. Therefore, information privacy and collaborative environments are two information system related concepts that are identified as priority research fields [2] and [3], vital to the continued and successful growth of many Information Communications and Technology (ICT) dependant industries.

Significantly improving information privacy protection and personal data management in collaborative environments provides many advantages to information requestors and information providers alike. Strong privacy controls are a major contributor to increased trust between member entities [4] which in turn can facilitate increased participation and contribution to a collaborative environment. As the collaboration grows so to does the need to ensure privacy is preserved along with clearly defined bounds of information flow for effective personal data management.

CE's by their very nature promote cooperation and the development of open and adaptive technologies [5]. Such environments present many interesting issues and challenges for information privacy and data security. Clarke [6] defines information privacy as being a combination of communications and data privacy. Formally defined as '… the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves' [6].

The focus of this paper is to provide a foundational perspective of our work investigating Information Privacy issues in the realm of collaborative environments. Information Privacy conformance needs to be integrated from system inception, but an effective privacy solution must be a symbiotic molding 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 collaborative environments. 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 the collaboration.

The rest of the paper follows a common structure outline as follows. Section 2 provides relevant background material on Information Privacy and research in this area. Additionally, a review of our previous work and publications in the field are discussed. Current collaborative environment approaches to Information Privacy and Data

Security is included in Section 3. Section 4 provides our proposals of the TLC Framework for Collaborative Environments and the importance of the TLC-PP framework for a Privacy Augmented Collaborative Environment (PACE). A brief conclusion and future work is provided in Section 5.

2 Background and Related Work

Modern privacy solutions are often derived from the application, both in combination and isolation, of the four main models of privacy protection [7]. The models listed in [7] are Comprehensive Laws, Sectoral Laws, Self Regulation, and Technologies of Privacy. Of interest to our own work is the impact of collaborative environments on information privacy and what modifications are required for privacy protections to operate effectively in collaborations. The reason being is that many of the technology of privacy solutions, that are proving to be the most popular form of protection, rely on varying levels of computationally secure methods, such as encryption, to provide security and privacy of personal data [8]. Our focus is on Information Privacy rather than Information Security, and specifically the development of a comprehensive collaboration wide approach to information privacy. From a technological perspective this involves the development and integration of Privacy Enhancing Technologies [8] with legislative, regulatory and social components. The uniqueness of privacy in terms of its subjective nature and openness to individual interpretation and representation has allowed it to evolve with similar advances in technology, society, culture and values [9]. 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 distributed collaborative environments. Therefore, a number of PETs make extensive use of encryption in some manner to help protect privacy. These include the Identity Protector [10], Shield Privacy [11], and Privacy Protector [12].

From a social privacy protection perspective 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. Collaborative environments assist in empowering small to medium enterprises to form transitory structures through collaboration. They not only facilitate knowledge transfer but also resource and expertise sharing. An ideal situation is to ensure that privacy best practices can be formulated and spread through out the collaboration by the sharing of resources. For example, one member of the collaborative community is recognized as providing good 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 a number privacy protecting purposes. One of the main objectives is to highlight potential threats to information privacy and any advantages that may be gained from the nature of collaborative environments. Another is the proposal of a framework to address the threats to privacy in collaborative environments. We show that many of these solutions will require a unique molding of technical, legal and community (social) elements to ensure information privacy.

3 Information Privacy Issues in Collaborative Environments

Advances in technology are providing valuable ways for entities to share information of any nature with others [13]. With increased sharing of information in addition to escalating methods of data collection it is imperative that adequate privacy practices are in place to protect and effectively manage entity personal data. Issues relating to uncertainty and establishing trust with 'unknown' entities produces additional risks when interacting with collaborative environments. Further, the inability to clearly determine the boarders of information flows within a collaborative environment contributes to user privacy concerns and complicates personal data management [14].

Privacy protection problems escalate in collaborative environments operating across multiple countries and regions. Due to the diverse and inconsistent legislative and regulatory global privacy landscape, enforcement and protection of privacy can be difficult in multi-national collaborations. For example a fictitious collaborative environment is represented with information system infrastructure located in six different countries all subject to very different privacy laws and regulations. That is, very different models of privacy protection are followed in the European Union (EU) compared to the United States. So while collaborations are adept at overcoming space and time obstacles for rapid knowledge sharing they are

currently very limited in managing and protecting privacy of personal information that may constitute part or all of the knowledge being shared. As stated in [15] organizations need to "… develop privacy policies and procedures that allow local privacy laws to be respected without restricting the global flow of information.".

Collaborative environments not only need to protect privacy but they must also effectively manage personal data transmitted in to, within, and out of the collaboration. Therefore, privacy protection in collaborative environments should be more concerned with how the data is used and ensuring an entity retains complete or significant control over their personal data. Hence, assistance in the form of tools, notifications and accessible information should be provided to members of the collaboration to enable better management of their privacy. Allowances should also be made for the individualistic and multi-dimensional nature of privacy by providing controls that can be configured by each entity depending on the situation. This will help accommodate the diversity and often dynamic conditions that are encountered within collaborative environments and likely to influence a member's privacy perception.

4 Technical, Legal, and Community - Privacy Protection Framework and a Privacy Augmented Collaborative Environment (PACE)

Research to date strongly indicates that no single model of privacy protection is sufficient to provide a complete information privacy solution [7]. Therefore, we propose that a solution to this issue is to develop systems and operating environments that integrate a symbiotic molding of all four models of privacy protection. In addition, privacy by design and information system Hippocratic principles [16, 17] 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 [18, 19] as well as social and cultural environmental conditions need to be accounted for within the framework during development, deployment and operation. Therefore, we propose a framework entitled Technical, Legal, and Community Privacy Protection (TLC-PP). It is an approach that combines all four models of privacy protection [7], as well as consideration for the influence of social and cultural ideals and perceptions from the collaborative environment community.

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 collaborations. The remainder of this section details each of the Technical, Legal, and Community privacy protecting components and our solutions within each component of the TLC-PP framework for collaborative environments. Due to space limitations a general outline and overview of solutions within each of the three components is provided. Readers are encouraged to read our additional related publications for more comprehensive discussion of our information privacy protecting solutions for collaborative environments.

4.1 Technical Privacy Protections

Technical privacy protections are frequently referred to as Privacy Enhancing Technologies (PETs). Common PETs include proxies and firewalls, anonymizers, Platform for Privacy Preferences Project (P3P), encryption tools, spam filters, cookie cutters, and automated privacy audits [20]. Since the initial demand for PETs their application and variety has increased significantly. They have come to represent more than technological support for personal data protection and now provide informational self-defense [21]. PETs now provide methods of protection for entities against many privacy invasive behaviors including unwanted surveillance and disruption. PETs in the context of our research have a broad scope, due to PETs not having a widely accepted definition, but their primary function is to minimize the exposure of private date for entities using electronic services within a collaborative environment. More generally the purpose of PETs is to protect the privacy of entities, while still enabling them to interact with other entities within a collaborative environment through digital mediums [22].

We recognize the importance of technologies of privacy and have made it one of the three critical framework components for comprehensive privacy protection. Our ongoing research has developed a number of technical solutions for enhancing entity privacy protection and personal data management. Each element is an integral part of the technical component of our TLC-PP framework. They are:

1) Shield Privacy: In order to meet space requirements interested readers are directed to [11] and [23] for the complete details of shield privacy. The technical methodology consists of four privacy by design and implementation rules. The rules guide the design and implementation of information

systems and collaborative environments to ensure information privacy and personal data management requirements are accommodated. The four rules are the following:

- PDM-ADM Design and Implementation Rule: Our approach to Personal Data Minimization (PDM) and Anonymous Data Maximization (ADM). PDM is used for determining and ensuring the minimum amount of personal information required by the collaboration or information system to function. ADM is used for determining and ensuring the maximum amount of personal information can be made anonymous for use throughout the collaboration or information system.
- SDD Design and Implementation Rule: Our approach to the Separation of Duty and Data (SDD) within the information system. SDD involves the segregation of system roles and data based on sensitivity, context of use, and entity assigned personal data access permissions for information requestors.
- HPP Design and Implementation Rule: Hippocratic Privacy Policies (HPP) is built upon the work proposed on Hippocratic Databases [18]. Hippocratic implies taking responsibility to ensure confidentiality and integrity of personal data. When applied to information systems and collaborative environments it infers that the information systems and collaborations take responsibility for the information privacy of entities using them and the protection of personal data they manage.
- Data Security Design and Implementation Rule: the latest data security technologies should be reviewed and continually integrated into the collaborative environment to ensure the protection of personal data at rest and in transit.

2) Privacy Using Graphs (PUG): PUG is a PET for managing privacy and personal data requests. The application uses directed weighted graphs to visually represent privacy, security, trust, and contextual relationships between entities in a collaborative environment. The two primary nodes of the dynamically generated graphs represent the starting node of the Information Provider (IP) and the final node of the Information Requestor (IR). When an IP receives a personal data request from an IR the IP can use the PUG application to generate a directed weighted graph mapping the 'social' or 'association' network from them to the IR. PUG requires an initial configuration by each member entity to appoint up to three 'trusted' member entities. Using the idea of 'six degrees of separation' a social or trust network of entities can be established for the collaboration. IP's can use this network to assist in visualizing personal data requests in order to determine whether they should be granted or denied. Again due to space limitations readers are directed to [24] for full details.

3) Fair Privacy Principles and Preferences (F3P): F3P is our unique contribution to privacy preference technologies. After identifying the absence of situational and compensation elements in current privacy preference technologies we addressed the problem by extending privacy preferences to include two new elements. We labeled the new elements SITUATION and REWARD. As privacy is widely accepted as being an individualistic notion meaning many different things to many different people then privacy preferences should reflect this. For an entity their perception of privacy and its worth changes with situation and possible compensation. Therefore, by allowing configuration of privacy preferences based on different situations and expected rewards they are more adept at catering for more unique individuals. Complete details of F3P are discussed in [18] and [25].

4.2 Legal Privacy Protections

We use the term Legal to encompass all types of legislative and regulatory privacy protection models. Multinational collaborative environments can be composed a host of different information systems governed by different privacy legislations and regulations. Ideally privacy policies and practices for a collaborative environment should be consistent for all member entities. Therefore our legal privacy protections focus on the development and production of uniform privacy laws, regulations, and policies based on best practice adoption or benchmarking. Each element is an integral part of the legal component of our TLC-PP framework. They are:

1) Privacy Evaluator Module (PEM): PEM is an XML based privacy legislation, regulation, and policy comparison tool. As collaborative environments can span multiple countries they are subject to a diverse set of privacy laws and regulations. We have developed an application that is able to compare the various privacy policies, based on a standard collaboration wide XML template, to identify differences. Information system stakeholders than are members of the collaborative environment are provided with the XML template to complete and submit to PEM. The XML privacy policy template is used to represent the information privacy legislations and regulations applicable to the information system in question. The templates are also structured in such a way that 'most complete' or 'most comprehensive' privacy policy can be

identified and set as the benchmark privacy policy and practices for the collaborative environment.
2) Manual Privacy Management (MPM): Through our own experiences and those documented in the literature we have acknowledged that the legal component of information privacy protection and personal data can not be completely automated with current technologies and operating environments. Therefore, in the absence of a globally enforceable uniform set of privacy principles and practices manual enforcement and monitoring is required. As part of our MPM solution we endorse the appointment of a Privacy Officer (PO) that is tasked with legal privacy protection management. The MPM also includes a detailed list of privacy objectives and guidelines for the PO to follow in the administration of privacy across the collaboration.
3) Privacy Benchmarked Policy (PBP): Through the application of PEM and practice of MPM a collaborative environment can produce a Privacy Benchmarked Policy (PBP) for use across the collaboration. The PBP is not necessarily the representation of a single member information systems privacy policy. The PBP should encompass all of the relevant privacy legislations and regulations applicable to all entities within the collaborative environment.

4.3 Community Privacy Protections

The element of Community Privacy Protection is perhaps the most important model in terms of the overall success of entity privacy acknowledgment and understanding. However, it is also the element faced with the most difficult challenges and the hardest tasks to successfully implement, as it is heavily reliant of many of the same sociological influences of privacy. Due to the very nature of the Community model it is very hard to develop tangible solutions that an entity can readily implement and integrate into a collaborative environment. The general premise is that the community of member entities that constitute a digital collaborative environment must acknowledge, understand, support, and encourage good information privacy and personal data management practices and protection. We address these issues through the provision of three solutions. Each element is an integral part of the community component of our TLC-PP framework. They are:
1) Privacy Awareness and Notification (PAN): PAN is a set of techniques, tools, and procedures for providing comprehensive privacy awareness and notification. Through the use of 'tools-tips', 'roll-overs', multi-layered contextual privacy policies, and privacy statements member entities of the collaboration are constantly presented with an abundance of privacy and personal data information. Additionally the PAN solution is implemented using readily available free web technologies present in most collaboration's.
2) Privacy Protecting - System Development Life Cycle (PP-SDLC): The PP-SDLC is an extension to the common system development life cycle that integrates detailed privacy protection guidelines and strategies throughout each phase of the methodology. The privacy protecting and personal data management guidelines are expressed in a straightforward and easy to comprehend manner to ensure all information system stakeholders are capable of completing the necessary privacy objectives and tasks detailed in PP-SDLC.
3) Community Observed Privacy (COP): COP represents policing by a collaborations stakeholders and users to instill and maintain a privacy protecting culture. Support is provided for anonymous logging of privacy violations or unsatisfactory privacy services to the Privacy Officer for follow up and action. It is a key solution in fostering an information privacy culture.

5 Conclusion

The Technical, Legal, and Community Privacy Protecting framework proposed in this paper provides a sustainable information privacy solution for collaborative environments. The three key components being Technical, Legal and Community models of protection each provide three unique privacy protecting and personal data management utilities for member entity use. The integration of application of the TLC-PP framework is a significant contribution towards the delivery of a Privacy Augmented Collaborative Environment (PACE). Our contribution is setting the PACE for sustaining privacy in autonomous collaborative environments.

References:

[1] K. Borcea-Pfitzmann, K. Liesebach, and A. Pfitzmann, "Establishing a Privacy-Aware Collaborative eLearning Environment," in Proceedings of the EADTU Annual Conference 2005: Towards Lisbon 2010: Collaboration for Innovative Content in Lifelong Open and Flexible Learning, Rome, November 2005.
[2] J. Feigenbaum and D.J Weitzner, "Report on the 2006 TAMI/PORTIA Workshop on Privacy and Accountability," Workshop on Privacy and

Accountability, Massachusetts Institute of Technology, MA USA, June 2006.

[3] I.L. Ballesteros, "New Collaborative Working Environments 2020," Report on industry-led FP7 consultations and 3rd Report of the Experts Group on Collaboration@Work, European Commission, February 2006.

[4] R. Clarke, "Privacy as a Means of Engendering Trust in Cyberspace," June 2001, http://www.anu.edu.au/people/Roger.Clarke/DV/eTrust.html.

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

[6] 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.

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

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

[9] 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.

[10] 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.

[11] 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.

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

[13] JJ. Cadiz and A. Gupta, "Privacy Interfaces for Collaboration," Technical Report MSR-TR-2001-82, Microsoft Corporation, 2001.

[14] M/Cyclopedia of New Media, "Virtual Communities – Privacy Issues," Creative Industries Faculty, QUT, http://wiki.media-culture,org.au/.

[15] J.B. Spira, "Privacy in the collaborative business environment," KM World, November 2004, http://www.kmworld.com/ReadArticle.aspx?ArticleID=9595.

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

[17] R. Agrawal, J. Kiernan, R. Srikant, Y. Xu, "Hippocratic Databases", 28th International Conference on Very Large Databases (VLDB), Hong Kong, 2002.

[18] 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.

[19] 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.

[20] L.F. Cranor, "The Role of Privacy Enhancing Technologies," Centre for Democracy and Technologies, March 2007, http://www.cdt.org/privacy/ccp/roleoftechnology1.shtml.

[21] G. Danezis, "An Introduction to Privacy Enhancing Technologies," presented at Internet Society Geneva's Monthly Conferences Cycle, Geneva, Switzerland, July 2004.

[22] Meta Group Report, "Privacy Enhancing Technologies," Ministry of Science and Technology, Denmark, March 2005.

[23] G. Skinner, S. Han, S. and E. Chang, E., "Shield Privacy: A conceptual framework for Information Privacy and Data Access Controls", WSEAS Transactions on Computers, Issue 6, vol. 5, June 2006, pp. 1375-1381.

[24] G. Skinner and M. Miller, "Managing Privacy, Trust, Security, and Context Relationships Using Weighted Graph Representations", WSEAS International Journal of Information Science and Applications, Issue 2, vol. 3, February 2005, pp. 283-290.

[25] G. Skinner, S. Han, and E. Chang, "Integration of Situational and Reward Elements for Fair Privacy Principles and Preferences (F3P)", in proceedings of IEEE International Conference on Industrial Technology (ICIT2006), Mumbai, India, December, 2006.