

A FRAMEWORK FOR IDENTIFYING CONFIDENTIAL INFORMATION IN A B2C E-COMMERCE INTERNET TRANSACTION

(Bob) Weihai He¹, Neville Williams¹

¹School of Informatics & Engineering
The Flinders University of South Australia

ABSTRACT: An extensive literature review on confidential information in a B2C e-commerce Internet transaction from three key perspectives of customers, businesses as well government and industry is presented in this paper. The literature review examines how customers perceive their confidential information, how businesses understand and provide solutions to protect the confidential information and how the Australian government's legislation and industry's self-regulation define the confidential information. Significant gaps in identifying confidential information among the three key perspectives are discussed. A framework is proposed for identifying confidential information in a B2C e-commerce Internet transaction by integrating the three key perspectives. The framework could be used by customers and businesses to identify confidential information in a consistent way. This paper is concluded by introducing possible future research issues.

INTRODUCTION

In a business-to-consumer (B2C) electronic commerce (e-commerce) context, Internet transactions are conducted between businesses and customers [Sch04]. E-commerce advances exchange of a large amount of information among its participants [Mao01]. The dramatic development of Internet technology requires confidential communications to be protected over the "open network" [WS96]. Confidentiality on the Internet has been defined on the basis that "only the sender and intended receiver should be able to understand the contents of the transmitted message" [KR03]. The definition of confidentiality in the e-commerce context has been given as "information that is private or sensitive should not be disclosed to unauthorized individuals, entities, or computer software process" [TK03]. A related but different concept is privacy. There are, however, different definitions of privacy in the literature. An early definition of privacy is "the right to be let alone" [WB90]. Another common definition is the "claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others" [Wes67]. A more recent definition of privacy is "the subject (owner) of information can *control* the information [AA03]. The last definition of privacy is used in this study.

The literature review presented in the following section examines how customers perceive their confidential information, how businesses understand and provide solutions to protect the confidential information and how the Australian government's legislation and industry's self-regulation define the confidential information. The review, however, reveals significant gaps of identification of confidential information among the three key perspectives. A framework for identifying confidential information in a B2C e-commerce Internet transaction by integrating the three key perspectives is proposed.

THREE KEY PERSPECTIVES

Customer's Perspective

Privacy has become a problem for online customers, since "the Internet has become a transmission line and repository for privacy information" [Law98]. In the e-commerce environment, there is often a "one-way mirror effect", that is, businesses ask customers to provide personal information, but customers have little knowledge about how their information will be used [CRA99]. There is, however, still a lack of standards for privacy protection in the online environment [AA03]. By taking the limitations and risks of current Internet technologies into account, there is often "confusion and mistrust" from customers in the e-commerce environment [CRA99].

Previous studies have reported the importance of understanding customer privacy concerns and found various factors that influence their concerns. A Roy Morgan [RM01] survey shows that the majority of participant customers claimed their privacy to be important. The customers' privacy

concerns are surveyed in-depth by Ackerman, Cranor and Reagle [ACR99] and Cranor, Reagle and Ackerman [CRA99], who examined a range of e-commerce scenarios of the participant customers' preferences about privacy. In both studies, a number of factors were identified as influencing customer privacy concerns. Recent studies by Arami *et al.* [ATPM04] and Bellman *et al.* [BJKL04] found that customer attitudes about privacy depended on a number of demographic factors such as gender, knowledge, and experience. The Office of the Victorian Privacy Commissioner [OVPC02] supports these findings and further reported other key influencing factors such as level of education and awareness of privacy legislation, age, nationality and ethnic background.

Research findings also suggest that customers could have problems in the understanding of several terms associated with "personal information" or "privacy". For example, a survey by Roy Morgan [RM01] in Australia found that respondent customers tended to use inconsistent and unclear definitions of the term personal information. When asked to define the term, the most common responses were: address (private/business), phone number (private/business), name and income details [RM01]. The health case notes, customer service information and personal opinions, which are defined by the legislation as personal information, were not mentioned by customers [RM01]. Moreover, a survey by the Office of the Victorian Privacy Commissioner [OVPC02] reports a study in the USA that found that customers meant different things when they talked about privacy. The survey found that for some Americans, privacy means anonymity, while for others it means confidentiality [OVPC02].

Business's Perspective

An understanding of customers' privacy concerns has become crucial for learning how to best collect and use individual customer's personal information [CBSL02]. The identification of confidential information requires the e-commerce businesses to provide solutions to secure each customer's confidential information.

Technology Solutions: Confidentiality in an Internet transaction is usually provided by encryption [Bhi96]. There are several existing mechanisms to secure transactions based on cryptography, including SSL (Secure Socket Layer) / TLS (Transport Layer Security), IPsec (IP Security) and VPN (Virtual Private Network). Although IPsec offers a global security to all applications, the complexity of IPsec comes from the requirements of an IPsec stack to be installed [ARH04]. Similarly, due to the dynamic and distributed nature of VPN, a sophisticated system is required [ARH04]. In contrast, SSL is "widely deployed and its embedded base will cause it to supersede any other session-layer protocols" [Bhi96]. Thus, SSL and TLS protocol have been widely implemented and is now regarded as the "de facto standard" for providing secure e-commerce transactions over the Internet [Cho02] [SBEW01].

Although SSL/TLS encrypts potentially strong security, (that is, the entire stream is protected), all material including materials which do not need to be secured, is protected to the same level [DJ99]. Thus, this approach has introduced significant performance constraints to the use of SSL/TLS. In addition, with SSL/TLS encryption, it is still possible to learn the IP address of the client and server machines and the length of data being exchanged [Gri04]. On the other hand, even though SSL/TLS support strong encryption during the Internet transaction, it could not guarantee the confidentiality of the message, because when the encrypted messages arrive at the server, they are all decrypted, which leaves the messages in plaintext [Cho02]. The privacy issue of database has also attracted the attention of the media. For instance, NineMsn [Nine05] reports that a worldwide incident in 2005 "appears to be the largest yet involving financial data in a series of security breaches affecting consumer data at the databases of major financial institutions". These findings indicated that the privacy of the Internet transaction and e-commerce database could not be ensured by just using encrypted transaction technologies like SSL/TLS [Bel05].

Privacy Policies & Technologies: Privacy policies specify under what conditions business can exchange and legitimately use customer personal information [KFPSSD04]. Each privacy policy, however, differs greatly because of the lack of standardisation across different industries and organizations [AEHSBJ04]. Privacy technologies that address customer's privacy concerns are introduced to facilitate the applications of privacy policies [Ack00]. The Platform for Privacy Preferences (P3P) is one of the privacy technologies which allow Web sites to convey their privacy policies in a computer-readable format [Cra03]. Another common technology, the Lucent Personal Web Assistant (LPWA), provides a pseudonym proxy for logging in to Web sites, "giving customers

consistent access to registration based systems without revealing potentially sensitive personal information” [Hoc00]. LPWA’s proxy-based design, however, tends to limit the server’s performance and decreases the overall reliability [Hoc00]. Fortunately, since P3P presents the privacy policy in a way that customers find easier to understand, its use could lead to other privacy improvements [Cra03]. For example, it could reduce the amount of information collected or secondary uses of that information [Cra03] [Ack00].

A number of research studies [Gho02] [Hoc02] [KS02] have demonstrated that P3P is not without problems. They found that the P3P is not backed up by privacy technologies that could enforce the promises in the e-commerce business. Moreover, the vocabulary of P3P technology used to convey information practice disclosures remains quite complex [Hoc00]. As a result, there could be “misinterpretations and confusions” in the use of P3P [Hoc00] [Fis01]. Moreover, Fischer-Hübner [Fis01] argues that P3P in practice could push or even force customers to give up their privacy. In addition, Anton *et al.* [AEHSBJ04] argue that P3P could force customers’ preferences and concerns into defined privacy categories, further limiting their options. Improvement of the privacy policies and technologies, thus, tends to reply on the better understanding customer privacy concerns.

Government & Industry’s Perspective

Although the introduction of privacy legislations would provide a degree of security for customers and encourage confidence in e-commerce business, the impact of the legislations requires businesses to undergo a “cultural change” [Mar02]. They require and possibly force the e-commerce business to change the way they understand and protect customer personal information.

Government Legislation: There is an established legislation in Australia that requires, as a matter of law, businesses to comply with the Privacy Act 1988 (covers public sector) and Privacy Amendment Act 2001 (covers a large parts of the private sector) [Mar02], when customers’ personal information is handled. The ten National Privacy Principles (NPPs) define the key obligations in respect to customer personal information [Als03]. The 1980 OECD Guidelines is one of examples of the internationalization of customer privacy protection [BJKL04]. The scope of international e-commerce and the nature of Internet technologies enable international cooperation to become a key aspect of the online protection of confidential information [APC03].

Greenleaf [Gre01] argues that the definition of personal information in the legislation could be problematic and may result in a severe effect on the applicability of the NPPs. The study revealed that it is not clear whether the email addresses or IP addresses constitute personal information [Gre01]. This argument is supported by Dixon [Dix01], who argues that the definition of “personal information is too broad” and “does not provide guidelines for privacy protection”. In contrast, the Australian Privacy Foundation [APF04] found that the definition of personal information to be limited. They argue that it is not clear if the legislation would cover, for example, “video images that have not been indexed by reference to individuals” [APF04]. In many countries, legislation could not keep up with the development of technologies, leaving serious gaps in protections [Ban99]. In Australia, nevertheless, Small and Medium Enterprise (SME) businesses are given certain exemptions from the privacy legislation [Mar02]. Thus, from the legislation perspective, there are either broad or limited definitions of the customer personal information, leaving the definitions of confidential information unclear to the customers and businesses.

Industry Self-Regulations: The privacy seal program is one of the industry’s self-regulation approaches to protect customer confidential information. A privacy seal on the Web site can be accessed by customers to receive visual confirmation of the Web site’s compliance with the privacy seal program’s standards [KM02]. Privacy seals programs aim to make customers more comfortable with Internet transactions and to ensure e-commerce Web sites keep their privacy promises [SKR02]. Thus, online privacy seals could create extra trust for the online customers [KSL04]. The three major privacy seal programs include, namely, TRUSTe, CPA WebTrust and BBBOnline. Privacy seal programs could complement privacy policies, because customers often a trust third party protection organization rather than relying on the full privacy policy [AK02]. Privacy seal programs have been used as “an alternative approach adopted by many e-commerce businesses in the absence of comprehensive privacy regulations” [RBE03].

Nevertheless, there could be problems with the design and effect of the privacy seal programs. They require an assessment of “fair information practice” on the e-commerce business. Such “fair

information practice”, however, could vary from industry to industry. The level of trust towards an e-commerce business could vary from one culture [Fuk95] to another. Demographical factors [CR04] also contribute to this variation. Another problem with privacy seals programs was found to be that they do not ensure real commitment to privacy protection, but only a compliance of Web site’s privacy statements with the assessment criteria of privacy seal programs [AK02] [MD03] [Moo05]. The question remains, however, whether the criteria adopted by the privacy seal programs meet the customer privacy expectations.

A PROPOSED FRAMEWORK

Issues of confidential information in B2C e-commerce introduce many challenges. A number of recent studies have surveyed the customer privacy issues [CR04] [CP04], technical solutions [CP02] [AGK03] [Gol03] [Lin05] [Sty05] and regulatory approaches [Fis01] [Pay04]. Discussions in previous sections, however, imply that there are potential problems in each of the three key perspectives:

- It appears from the surveys that the concepts of “personal information” or “privacy” may not be fully understood by customers. Without comprehensively understanding confidential information from customer’s perspective, validity of the surveys would be limited.
- The P3P specification makes numerous assumptions about how customers perceive privacy [RC99]. Privacy policy creation and customer privacy concerns are often found inconsistent with each other [EA04]. Unlike the heavy SSL/TLS “encrypts everything approach”, there is an opportunity to apply the XML Encryption technology to partially encrypt selected elements to be secured [Gee03] in order to minimize performance penalties [Men03].
- The nature of legislation constrains its specific definition of confidential information. As a result, businesses and customers may find it difficult to follow the legislation. In addition, so far, customers could only passively accept the Web site’s privacy policy or recognize the online seal programs [CP04]. This situation, however, contradicts the requirements of privacy, which claims *control* over customer’s confidential information.

The literature review further demonstrates that there are significant gaps in the identification of confidential information from the perspectives of customers, business as well government and industry. The three key perspectives might have not adopted a consistent identification of confidential information (or its related concepts). Without a consistent understanding of the concept, however, any protection approaches of confidential information tends to be compromised. Early steps in the construction of a suitable framework for identifying confidential information in a B2C e-commerce Internet transaction are proposed below.

Firstly, a data element from the business and customer perspective is classified into categories of confidential information. The data element could be single customer information value (for example, customer names). Confidential information in different categories represents different priorities to protect. The classification is based on the philosophy that “not all personal information is equal” [Ber00]. Criteria used in the classification are mainly based on the concept of “inference problem” [FJ02] and “level of linkability to its data subject” [KS02]. The classification incorporates a number of definitions of “personal (identifiable) information” [GS01] [Gre01] [Gol03] [RBE03] [Lin05] “private information” [GS01]; “privacy” [ATPM04] [CP02] [Gho02] [Fis01]; “aggregate or statistical information” [Fis01] [GS01]. There are three categories of confidential information in the framework, namely, Identifiable or Identified Information (III), Related Identifiable Information (RII) and General Identifiable Information (GII). Other data not falling into any of these categories has no confidential considerations and may be excluded.

- The *Identifiable or Identified Information* is considered as unique, identifiable and identified for a customer. Examples include Social Security Number (SSN), Medicare number, credit card number and so on. Information classified at this level is very important to be protected, because they always act like “keys” to the many external databases, for instance, the bank databases held by the financial institutes [Ber00].
- The *Related Identifiable Information* could be used in combinations to identify a customer. Examples are customers’ (first and last) names, (business and home) addresses, (business and

home) phone numbers and so on. Although in certain contexts, any of the RII information could uniquely identify a person, the combinations of two or more of them would increase the chance of the identification.

- The *General Identifiable Information* can be used to identify a customer by using a combination of RII and GII. For example, the combinations of GII (birthday) and other RII (postcode) would be used to increase the chance of identifying a particular person [GS01].

A conceptual overview of the classification of confidential information is shown in Figure 1 (a). The III, RII and GII are shown in three levels, which suggest an analogy with the famous Orwell quote “all animals (data) are equal, but some animals (data) are more equal than the others” [Orw45].

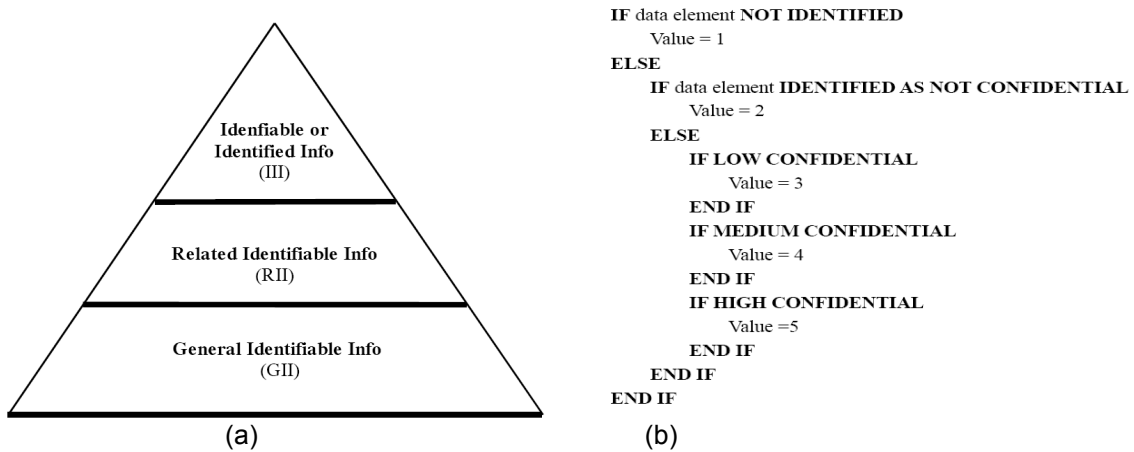


Figure 1 – A Conceptual Classification of Confidential Information

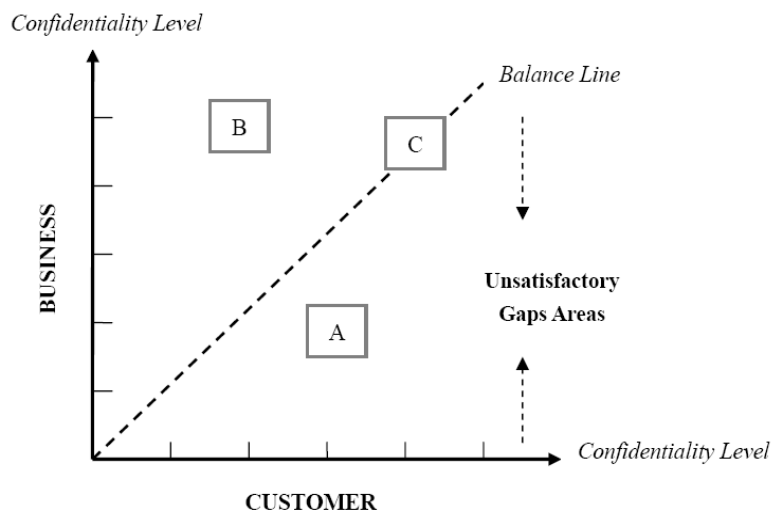


Figure 2 – A Diagram of Identifying Confidential Information Gap

Secondly, in a B2C ecommerce environment, a customer could enter the confidential level (for example, medium or high) associated with the data element via a Web browser, while business could specify the level in their business privacy policy. The confidentiality levels will then be determined by an algorithm to determine the customer and business expectations of confidential level for a given data element. A quantifying algorithm shown in Figure 1(b) is applied for each data element. The data element is assigned value of 1 if it is not identified (either neglected or not applicable). If the data element is defined but not identified as confidential, then a value of 2 is assigned. In other cases, the values 3 to 5 will be given based on the level, including low, medium or high provided.

Thirdly, the value obtained from quantifying algorithm is translated to the diagram presented in Figure 2 to determine the extent of the gap between actual (business) and expected (customer) levels of confidentiality. After obtaining both the value from customer and business perspective, an offset could be obtained and shown in the diagram. Offset falls on the balance line (C in Figure 2) represents a match between the customers and business for the level of confidentiality of a certain data element. When an offset falls above the balance line (B in Figure 2), business places a higher level of confidentiality over the customer concerns. The main problem occurs, however, when the offset falls below the balance line (A in Figure 2). The “unsatisfactory gaps areas” represents the gaps where business did not match the customers concerns for a given data element.

CONCLUSION AND FUTURE RESEARCH

The framework presented attempts to identify the confidentiality factors involved in assessing the privacy levels of data element that can be seen in a typical B2C e-commerce transaction. The combination solutions of the three key perspectives remain the future direction of confidential information protection [CP02] [Gol03]. The gaps in confidential information identified by the proposed framework could minimise possible inconsistency problems that occur in the combination approach. Future research would include more detailed criteria for the classification of confidential information. The quantifying algorithm and the diagram would also be complemented with detailed guidelines. As pointed out by Linn [Lin05], Stytz [Sty05] and Rezgui *et al.* [RBE03], the goal of future privacy protection would focus on presenting confidential information in a form that remains protected under customer’s control. Thus, the application of the framework would aim to provide guidelines for the customers to better understand their confidential information in the B2C e-commerce context. In addition, guidelines from the framework could complement the design of privacy technologies, for example, P3P. Future research is needed on how to integrate the framework guidelines with the XML Encryption design, which encrypts partial confidential information to increase the overall performance. Whether the framework is a suitable tool to be used for guiding the development of privacy policy by business needs to be empirically established.

ACKNOWLEDGEMENT

We would like to thank Dr. Salah Kutieleh for his help in reviewing this paper.

REFERENCES

- [AA03] I. Araujo and I. Araujo. Developing trust in Internet commerce. *Proceedings of Conference of the Centre for Advanced Studies on Collaborative Research*, pages 1-15, 2003.
- [Ack00] M. Ackerman. Developing for privacy: civility frameworks and technical design. *Proceedings of 10th Conference on Computers, Freedom & Privacy*, pages 19-23, 2000.
- [ACR99] M. Ackerman, L. Cranor and J. Reagle. Privacy in e-commerce: examining user scenarios and privacy preference. *Proceedings of the 1st ACM Conference on Electronic Commerce*, pages 1-8, 1999.
- [AEHSBJ04] A. Anton, J. Earp, Q. He, W. Stufflebeam, D. Bolchini, and C. Jensen. Financial privacy policies and the need for standardization. *IEEE Security & Privacy*, 2(2): 36-45, 2004.
- [AGK03] J. Argyrakis, S. Gritzalis and C. Kioulafas. Privacy enhancing technologies: a review. *Lecture Notes in Computer Science*, vol. 2793, pp. 282-287. 2003.
- [AK02] N. Ashrafi and J. Kullboer. Data privacy: U.S. common practices. *Proceedings of the 13th International Workshop on Database & Expert Systems Applications*, pages 488-492, 2002.
- [Als03] N. Alston, M. Curran, S. Frost, O. Ganopolsk, C. Graham, M. Hall, G. Hughes, R. Jordan, J. Napoli, B. Scott, G. Stals, D. St Clair, S. Thorp, A. Tyree and N. Willmott. *E-Commerce law: a handbook for business*, LexisNexis Butterworths, 2003.
- [APC03] H. Aljifri, A. Pons and D. Collins. Global e-commerce: a framework for understanding and overcoming the trust barrier. *Information Management & Computer Security*, vol. 11, 2/3, pages 130-138, 2003.

- [APF04] Australian Privacy Foundation. *Review of Privacy Act 1988 private sector provisions submission by the Australian Privacy Foundation*, 2004, URL: <http://www.privacy.org.au/Papers/OFPCPteSectReview0412.doc> , Accessed: 20 June 2005.
- [ARH04] L. Alchaal, V. Roca and M. Habert. Managing and securing Web services with VPNs. *Proceedings of the IEEE International Conference on Web Services*, pages 236-244, 2004.
- [ATPM04] M. Arami, H. Treiblmaier, A. Pinterits and M. Madlberger. Information privacy concerns and e-commerce: an empirical investigation. *Proceedings of the 10th Americas Conference on Information Systems*, pages 1178-1189, 2004.
- [Ban99] D. Banisar. Privacy and data protection around the world. *Proceedings of the 21st International Conference on Privacy & Personal Data Protection*, 1999, URL: <http://www.pco.org.hk/english/infocentre/conference.html>, Accessed: 2 May 2005.
- [Bel05] S. Bellovin. Security and privacy enemies or allies. *IEEE Security & Privacy*, **3**(3): 92, 2005.
- [Ber00] H. Berghel. Identity theft, social security numbers and the Web. *Communications of the ACM*, **43**(2):17-21, 2000.
- [Bhi96] A. Bhimani. Securing the commercial Internet. *Communications of the ACM*, **39**(6): 30-35, 1996.
- [BJKL04] S. Bellman, E. Johnson, S. Kobrin and G. Lohse. International differences in information privacy concerns: a global survey of customers. *Information Society*, **20**: 313-324, 2004.
- [CBSL02] J. Cazier, C. Benjamin, B. Shao and R. Louis. Personal privacy preferences in e-business: a focus on trust and value compatibility. *Proceedings of the 8th Americas Conference on Information Systems*, pages 2204-2212, 2002.
- [Cho02] W. Chou. Inside SSL. *IEEE IT Professional*, **4**(4): 47-52, 2002.
- [CP02] W. Chung and J. Paynter. Privacy issues on the Internet. *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, pages 193-202, 2002.
- [CP04] J. Chen and Y. Park. Trust and privacy in electronic commerce. *Proceedings of the IEEE International Conference on e-Technology, e-Commerce & e-Services*, pages 117-120, 2004.
- [CR04] K. Chen and A. Rea. Protecting personal information online. *Journal of Computer Information Systems*, **44**(4):85-93, 2004.
- [Cra03] L. Cranor. P3P: making privacy policies more useful. *IEEE Security & Privacy*, **1**(6): 50-55, 2003.
- [CRA99] L. Cranor, J. Reagle and M. Ackerman. Beyond concern: understanding net user's attitudes about online privacy. *AT&T Lab-Research Technical Report TR 99.4.3*, 1999. URL: www.research.att.com/resources/trs/TRs/99/99.4/99.4.3/report.htm, Accessed: 1 April 2005.
- [Dix01] T. Dixon. Preparing for the new privacy legislation. *Cyberspace Law Resources*, vol. 43, 2001, URL: <http://www.nswscl.org.au/journal/43/Dixon.html> , Accessed: 5 May 2005.
- [DJ99] P. Dymond and M. Jenkin. WWW distribution of private information with watermarking. *Proceedings of the 32nd Annual Hawaii International Conference on System Sciences*, pages 5031-5039, 1999.
- [EA04] J. Earp and A. Antón. Addressing end-user privacy concerns. *Proceedings of the 10th Americas Conferences on Information Systems*, pages 1170-1177, 2004.
- [Fis01] S. Fischer-Hübner. IT security and privacy: IT privacy in the global information society. *Lecture Notes in Computer Science*, vol. 1958, pages 5-33, 2001.

- [FJ02] C. Farkas and S. Jajodia. The inference problem: a survey. *ACM SIGKDD Explorations Newsletter*, **4**(2): 6-11.
- [Fuk95] F. Fukuyama. *Trust: the social virtues and the creations of prosperity*, Free Press, 1995.
- [Gee03] D. Geer. Taking steps to secure Web services. *IEEE Computer*, **36**(10): 14-16, 2003.
- [Gho02] A. Ghosh. Maintaining privacy in an online world. *IEEE IT Professional*, **4**(5): 24-28, 2002.
- [Gol03] I. Goldberg. Privacy-enhancing technologies for the Internet II: five years later. *Lecture Notes in Computer Science*, vol.2482, pages1-12. 2003.
- [Gre01] G. Greenleaf. Privacy sector privacy: problems of interpretation, *the New Australian Privacy Landscape Seminar*, Faculty of Law, University of New South Wales, 14 March 2001, URL: <http://austlii.edu.au/~graham/CyberLRes/2001/3/> , Accessed: 5 May 2005.
- [Gri04] S. Gritzalis. Enhancing Web privacy and anonymity in the digital era. *Information Management & Computer Society*, vol. 12, 2/3, page 255-288, 2004.
- [GS01] S. Garfinkel and G. Spafford. *Web security, privacy and commerce*, O'Reilly Press, 2001.
- [Hoc00] H. Hochheise. Principles for privacy protection software. *Proceedings of the 10th Conference on Computers, Freedom & Privacy*, pages 69-72, 2000.
- [Hoc02] H. Hochheiser. The platform for privacy preference as a social protocol: examination within US policy context. *ACM Transactions on Internet Technology*, **2**(4): 276-306, 2002.
- [KFPSSD04] L. Kagal, T. Finin, M. Paolucci, N. Srinivasan, K. Sycara and G. Denker. Authorization and privacy for semantic Web services. *IEEE Intelligent Systems*, **19** (4): 50-56, 2004.
- [KM02] K. Kimery and M. McCord. Third-party assurances: the road to trust in online retailing. *Proceedings of the 35th Hawaii International Conference on System Sciences*, pages 175-185, 2002.
- [KR03] J. Kurose and K. Ross. *Computer networking: a top down approach featuring the Internet*, 2nd edition, Sydney Pearson Education, 2003.
- [KS02] G. Karjoth and M. Schunter. A privacy policy model for enterprise. *Proceedings of the 15th IEEE Computer Security Foundations Workshop*, pages 271-281, 2002.
- [KSL04] D. Kim, C. Steinfield and Y. Lai. Revisiting the role of Web assurance seals in consumer trust. *Proceedings of the 6th International Conference on Electronic Commerce*, pages 280-287, 2004.
- [Law98] G. Lawton. The Internet's challenge to privacy. *IEEE Computer*, **31**(6): 16-18, 1998.
- [Lin05] J. Linn. Technology and Web user data privacy: a survey of risk and countermeasures. *IEEE Security & Privacy*, **3**(1): 52-58, 2005.
- [Mao01] E. Mao. Electronic commerce: a framework development and some global implications. *Journal of Management Systems*, **15**(3): 27-36, 2001.
- [Mar02] A. Mark. *E-Business, the law and you*. Pearson Education Australia, 2002.
- [MD03] T. Moores and G. Dhillon. Do privacy seals in e-commerce really work. *Communications of the ACM*, **46**(12):265-271. 2003.
- [Men03] D. Menascé. Scaling the Web. *IEEE Internet Computing*, **7**(3): 84-87, 2003.
- [Moo05] T. Moores. Do consumers understand the role of privacy seals in e-commerce. *Communications of the ACM*, **48**(3): 86-91, 2005.

- [Nine05] NineMsn. Australian hit by US credit card breach. *NineMsn News*, 2005. URL: <http://news.ninemsn.com.au/article.aspx?id=9782> , Accessed: 10 July 2005.
- [Orw45] G.Orwell. *The animal farm*. The University of Adelaide Library Electronic Collection, 1945. URL: <http://etext.library.adelaide.edu.au/o/orwell/george/o79a/index.html>, Accessed: 1 July 2005.
- [OVPC02] Office of the Victorian Privacy Commissioner. *Guidelines to information privacy principles 2002: part 1: Overview, Collection Use and Disclosure*. 2002. URL: [http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/F1A1DFC7539A03A9CA256C52002D3640/\\$FILE/Guidelines_11_June_2002.pdf](http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/F1A1DFC7539A03A9CA256C52002D3640/$FILE/Guidelines_11_June_2002.pdf) , Accessed: 15 May 2005.
- [Pay04] J.Payne. Regulation and information security: can Y2K lesions help us. *IEEE Security & Privacy*, 2(2):58-61, 2004.
- [RBE03] A. Rezgui, A. Bouguettaya and M. Eltoweissy. Privacy on the Web: facts, challenges and solutions. *IEEE Security & Privacy*, 1(6): 40-49, 2003.
- [RC99] J. Reagle and L. Cranor. The platform for privacy preferences. *Communications of the ACM*, 42(2): 48-55, 1999.
- [RM01] Roy Morgan. *Privacy and business 2001*. Roy Morgan Research for Office of Federal Privacy Commissioner, 2001, URL: <http://www.privacy.gov.au/publications/rbusiness.html> , Accessed: 4 May 2005.
- [SBEW01] M. Steiner, P. Buhler, T. Eirich and M. Wainder. Secure password-based cipher suite for TLS. *ACM Transactions on Information and System Security*, 4(2):134-157, 2001.
- [Sch04] G. Schneider. *Electronic commerce: the second wave*, 5th edition, Thomson, 2004.
- [SKR02] N. Sivasailam, D. Kim and H. Rao. What companies are(n't) doing about Web site assurance. *IEEE IT Professional*, 4(3): 33-40, 2002.
- [Sty05] R. Stytz. Protecting personal privacy: hauling down the Jolly Roger. *IEEE Security & Privacy*, 3 (4): 72-74, 2005.
- [TK03] E. Turban and D. King. *Introduction to e-commerce*, Pearson Education, 2003.
- [WB90] S. Warren and L. Brandeis. The right to privacy. *Harvard Law Review*, 4(5):193-220, 1890.
- [Wes67] A. Westin 1967. *Privacy and Freedom*, Atheneum, 1967.
- [WS96] D. Wagner and B. Schneier. Analysis of the SSL 3.0 protocol. *Proceedings of the 2nd USENIX Workshop on Electronic Commerce*, pages 29-40, 1996.