December 2002

Effective Online Privacy Policies

Sharman Lichtenstein
Deakin University

Paula Swatman
University of Koblenz, Germany

Kanchan Babu
Deakin University

Effective Online Privacy Policies

Sharman Lichtenstein[1], Paula M C Swatman[2] and Kanchan Babu[3]

[1]School of Information Systems
Deakin University
Melbourne, Australia
slichten@deakin.edu.au

[2] Faculty of Informatics
University of Koblenz, Koblenz
Germany

and

School of Information Systems
Deakin University
Melbourne, Australia

[3]Telstra Retail
Melbourne, Australia

Abstract

Online privacy policies are important mechanisms for informing consumers about the level of information privacy protection afforded when visiting websites. To date, societal mechanisms and technologies have been the focus of attempts to improve the quality and effectiveness of these policies. Little attention, however, has been given to the development and use of organisational measures for this purpose. We present findings from an empirical study, including a set of organisational guidelines for effective online privacy policies, which extend the research base in this area and, more immediately, will assist companies concerned about the impact of privacy concerns on consumer web usage.

Keywords

IS Security, IS Policy, Managing IS, Risk

INTRODUCTION

Information privacy addresses the legitimate collection, use and disclosure of personal information, as well as "the interest an individual has in controlling, or at least significantly influencing the handling of data about themselves" (Clarke, 1999). Online privacy is increasingly acknowledged as a significant factor in e-Business success (Agre and Rotenberg, 1997; Bingi *et al*., 2000; Cranor *et al*., 2000; Hoffman *et al*., 1999; Privacy and American Business, 2002; Westin, 2001), with consumer concerns centring on "intrusions, manipulation, and discrimination; on special concerns about third parties capturing the sensitive self-revelations users are making on the internet; and on concerns about identity theft and stalking through capture of personal information" (Westin, 2001).

The online privacy policy (OPP) (or 'privacy statement') is a key organisational measure for assuring online information privacy for consumers, articulating the manner in which a company collects (online), uses and protects data, and the choices offered to online consumers for exercising their rights with respect to the use of their own personal information (Babu, 2000; Chung and Paynter, 2002; OPA, 2002). OPPs are intended to represent fair information privacy practices as first defined by OECD (1980), and later extended and modified to accommodate perceived e-Business, national and globalisation needs (see for example NPP, 2000; FTC, 2000).

Previous investigations of Australian and American OPPs have highlighted their ineffectiveness, revealing that many users consented to, or declined, policies unread – and that in general, policies were unclear, inconsistent with actual privacy practices, and poorly linked to business strategy and operations (Anton and Earp, 2001; Babu, 2000; Culnan, 1999; anonymous, 2000; EPIC, 1999; FTC, 2000; Freehills, 2000; Privacy and American Business, 2002). Encouragingly, there have been recent reports of improvement in policy

quality and prevalence, possibly due to various levels of regulation and/ or increased media attention given to the issues (Anderson, 2001; Adkinson *et al*., 2002). Nonetheless, the role of ineffective OPPs in the unabated stream of online privacy incidents continues to be observed (for example Mainelli, 2002).

Societal and technological support for OPPs is available, in various forms. The European Union established fairly stringent privacy legislation some years ago, in the process setting strict privacy requirements for other countries who wished to do business with them. In Australia, co-regulation is a recent approach to the issues, while in the US, industry self-regulation remains on trial, although future legislation appears likely. Various sets of privacy principles underpin these governmental initiatives to improve OPPs – for example, FTC (2000) in the US, and NPP (2000) in Australia. On a much smaller scale, independent third party assessment and verification of policies provides a level of policy assurance, via seal programs such as TRUSTe, independent audits and privacy certification (for example APCC, 2001).

New online privacy technologies may prove useful – for example, P3P, which enables users to view a technologically-translated version of an OPP in more usable form, as well as matching the policy to user-preferred privacy levels and informing users if policy privacy levels are inadequate for their needs (Reagle and Cranor, 1999; W3C, 2002). However to date, there has not been a significant uptake by companies of this approach, and future effectiveness of this solution is therefore uncertain (Harvey and Sanzaro, 2002).

Organisations can elect not to rely upon societal and technological measures, by employing organisational methods for guiding the development and support of their OPPs. However, we believe current organisational guidelines are not appropriate for this purpose. Most existing guidelines are fundamentally, national fair information practice principles (for example FTC, 2000; NPP, 2000; OPA, 2002), and were developed from professional expertise, rather than through rigorous research methods. These guidelines may therefore have missed some of the issues. Richmond (1999) developed an early set of guidelines based largely on case study research, and not taking into account nascent regulations or existing policies. Anton and Earp (2001) studied a set of health privacy policies, resulting in a taxonomy of OPPs, although this did not account for contextual issues or usability. Babu, in 2000, found existing guidelines to be inadequate in a variety of ways. Moreover, continued frequent occurrences of online privacy incidents suggest that existing OPPs are ineffective in managing the risks, possibly due to deficiencies in current sets of guidelines.

Our aim in this paper is to identify a set of organisational guidelines to use in the development of effective OPPs. Following this brief survey of the literature and current research into online privacy protection, we overview our research methodology. We then provide a set of guidelines for effective online privacy policy – drawing on a longitudinal study of online privacy policies conducted in 2000 and 2002. Finally, we present our findings and conclusions, suggesting avenues for further research.

RESEARCH METHODOLOGY

This study was conducted in two stages, two years apart. In the first stage (Babu, 2000), a literature review was employed to develop an initial model of guidelines for OPP. Next, a critical analysis of OPPs residing on the websites of eight American businesses and two Australian businesses was performed. The sites were: ebay.com, cdnow.com, 247realmedia.com, colesonline.com.au, wishlist.com.au, travel.com, disney.com, toysmart.com, craftshop.com, and realnetworks.com. These constitute five retail, one auction service, one travel and three entertainment companies. The sites were chosen because they were highly active and recognised e-Business sites at the time of study, and also featured substantial OPPs.

The ten policies were content analysed for guideline compliance, as indicated by a reasonable implementation of the guideline within the policy. Each policy was also analysed contextually, taking into account the influence of HCI, organisational, societal and other factors. A cross-policy analysis enabled the identification of trends, patterns and differences. An in-depth case study of a recognized Australian online retailer – termed OzeSale – was

conducted. As a result of these empirical investigations, the initial set of guidelines for OPP was revised.

In the second stage of this project – our extension in 2002 of the original investigations from 2000 – we reviewed the original as well as recent literature, reanalysed the original research data, and reviewed the original guidelines and results. We then content analysed the nine still existing OPPs in their updated forms in April, 2002 (including OzeSale's site OPP) for guideline compliance and contextual issues – again identifying trends, patterns and differences. Thus we arrived at a final set of guidelines for effective OPPs, and our research findings.

Due to the constraints of paper size, we are unable to include in this paper the substantial literature review underpinning our guidelines (which were revised as a result of our empirical work, as described above). We refer the interested reader to Babu (2000) for a comprehensive review of the relevant literature.

RESULTS AND DISCUSSION: GUIDELINES FOR ONLINE PRIVACY POLICY

In this section, we provide and discuss[1] a comprehensive set of high level guidelines for online privacy policy (Table 1), in the following categories: *awareness, data quality, security, information movement, user identification, accountability, user access, assurance, contact, choice, change management, children's privacy, sensitive information and exceptions* (compiled from Anton and Earp, 2001; Babu, 2000; FTC, 2000; NPP, 2000; and our additional investigations in 2002).

Online Privacy Policy Guideline Category	**Brief Description of Guideline Category**	**Guideline Within Category**
1. Awareness	The site should facilitate user awareness of its online privacy policy.	1.1 Prominence/ openness 1.2 Language 1.3 Notification 1.4 Classification 1.5 Collection 1.6 Purpose/ use 1.7 Disclosure 1.8 Consumer education 1.9 Third party involvement
2. Data quality	Personal information should be maintained as complete, timely and accurate, by the company.	
3. Security	Personal information should be secured wherever possible.	3.1 Data security 3.2 Data transmission 3.3 Cookies
4. Information movement	Details of personal privacy provided in various states of information movement should be provided to the user.	4.1 Information monitoring 4.2 Information aggregation 4.3 Information storage 4.4 Information transfer 4.5 Information disposal 4.6 Information personalisation 4.7 Transborder data flow

[1] Further details of the individual guidelines are available in a forthcoming journal article, currently under review.

Online Privacy Policy Guideline Category	Brief Description of Guideline Category	Guideline Within Category
5. User identification	Use and disclosure of a user's site identifier as personally identifiable information (PII), anonymous, or pseudonymous, should be stated.	5.1 User identifier 5.2 Anonymity 5.3 Pseudonymity 5.4 Nonrepudiation
6. Accountability	Company and user should be held accountable for actions.	6.1 Enforcement 6.2 User responsibilities
7. User access	Users should have opportunity to participate in their personal information protection, as necessary.	7.1 User access and self-correction 7.2 User access to other user data
8. Assurance	The policy should state ways in which companies assure users it is following its OPP in practice.	8.1 User recourse 8.2 Verification 8.3 Consequences
9. Contact	The policy should state how, and for what purpose, organisations contact users using PII to make the contact.	
10. Choice	The user should be given choices in respect to collection and use of personal information.	10.1 Consent
11. Change management	A company should state procedures for change management of its OPP.	11.1 Evolution 11.2 Changes to policy 11.3 Change of company control
12. Children's Privacy	The policy should provide information regarding access by, and involvement of, children.	
13. Sensitive information	The ways in which sensitive information (e.g. religion) is treated differently to other personal information, should be explained.	
14. Exceptions	Exceptions to the policy should be clearly stated.	

Table 1: Summary of guidelines for online privacy policy (compiled from Anton and Earp, 2001; Babu, 2000; FTC, 2000; NPP, 2000; **and our investigations in 2002)**

Our set of guidelines is intended as a roadmap for businesses, to ensure that all important areas are addressed in the development of OPPs. We point out that not all the guidelines included in our set are addressed by various national regulations, although our study suggests that all our guidelines are important, and therefore worthy of inclusion in our final set. We also note that there is, at present, some degree of overlap in our classification scheme.

Overall, we found that the OPPs studied in 2002 had improved in quality since 2000 – a trend which we attribute mainly to increased consciousness of online privacy issues within the e-Business community, combined with co-regulation or industry self-regulation based on recognised fair information practice principles. However, despite our finding of overall improvement in policy quality, we found that a significant portion of the guidelines in our set were inadequately addressed or missing, in many of the OPPs in 2002. Following, we discuss issues arising from our study of the nine policies and case study. For discussion purposes, we group the guidelines under the following headings: *awareness, data quality and security, information movement, user identification and accountability, user participation, change* and *special cases*. In the interests of paper size, we have limited the discussions to selected aspects, only[2].

[2] Further details of the individual guidelines are available in a forthcoming journal article, currently under review.

Awareness

A company has a duty to promote consumer awareness of online privacy issues resulting from a site visit. We found that overall awareness provisions have improved over the two years of the study, but suggest there is ample room for further improvement. Although most companies in both years posted a clearly labelled link to the OPP in a conspicuous manner and position on each page, this feature was rarely offered at the time of consumer need – for example, when personal information was being collected. Another aspect of awareness is the quality of language in which the policies are written – which the user would clearly wish to be simple, and easily comprehensible. However, language used by most policies in both years was generally complex and legalistic, while the structure and layout of information precluded understanding. An encouraging sign was that policy expression and comprehensibility improved in about half the sites over the two-year period – a promising trend.

Provision of awareness of the type of collected personal information – as well as the purpose for collection and disclosure or other use – was scarce in both years. Only a few policies provided any detail about personal information collected. As an example of the generality and informality we encountered in this regard, one policy stated: "Depending on what you purchase, we may also need to collect other personal information, like your clothing size." In contrast, eBay featured a very informative, comprehensive, personal information access chart, with each field of collected personal information plotted against third parties granted the specified accesses. There was minimal linking of specific, collected personal information to the purpose for which it was being collected, although there was linking of collected personal information overall to generic purposes such as "improved personalised service". Other than such generalised advice, several policies provided long lists of general uses of personal information. Advice regarding conditions of disclosure of collected personal information was confusing at all sites, in both years. In one OPP we found, "We'll never share that information with third parties interested in e-mailing you". This, of course, did not preclude collected personal information from being shared with third parties with interests other than emailing the user – for example, the placing of pop-up advertisements on the user's computer.

Providing awareness of the privacy issues involved in OPPs through consumer education, was limited in all cases to hyperlinks to third party consumer privacy advocate groups, such as EPIC and Online Privacy Alliance. The number of sites carrying out such linking, as well as the number of links provided, increased over the two year period. Despite these signs of improvement, we believe that much more than links of this type is needed for effective consumer education.

One area of improvement noted over the two-year period was policy notification of third party privacy levels, although most sites were providing this only through disclaimers, thereby divesting themselves of all responsibility for third party privacy assurance – a situation which clearly needs redressing.

Data quality and security

Data quality provision and assurance improved over the two-year period. The provision of consumer access to check and correct personal information increased over the two years, although in most such cases, only a contact email address, phone number or postal address were provided, rather than an online form. Several sites did provide online forms, however. There was no other provision of data quality assurance for personal information once the company had collected the data, other than security (see below). In all situations, all responsibility for data quality assurance rested with the user via personal information access, checking and correction, with no quality being assured by the company other than security assurances, as follows.

Security assurances increased markedly over the two-year period. Five OPPs in 2000, increasing to all in 2002, provided some commitment to data security – advising consumers of the use of SSL, firewalls and other security technologies, via corresponding symbols such as padlocks displayed on the sites. General security assurance statements were commonly found in OPPs – for example, "We employ many different security techniques to protect such

data from unauthorized access by users inside and outside the company". General disclaimers were also popular – for example, "However, perfect security does not exist on the Internet" and "…does not ensure or warrant the security of any information you transmit to us or from our online products or services, and you do so at your own risk".

The improvement observed over the two years suggests that companies appear to have recognised the need for reassuring consumers about the security of collected personal information. Nevertheless, the companies still adopted a cautious approach, issuing disclaimers about the security of any collected data while in transmission across the internet, pointing to the recognised vulnerability of the internet itself. This, however, represented an improvement over the situation in 2000, when none of the policies provided any information about the security of personal information while in transmission.

Information about cookies (where they were used) explaining their operation and use for tracking user activity, was too abbreviated for uninformed or inexperienced consumers, many of whom may experience difficulties in understanding text-only explanations. We suggest that another medium – for example graphics – could be useful to better explain this commonly used feature of websites.

Information movement

Information privacy protection should be provided during all stages of personal information movement through its lifecycle from collection until disposal, with the consumer being informed accordingly, through the OPP.

Currently, it is difficult for a user to ascertain the level or nature of tracking (typically via cookies) or personal information aggregation, from the confusing explanations given. It would be useful to investigate alternative methods for conveying these complex concepts more clearly. Advice as to what became of personal information once it had entered data warehouses was largely missing in both years in all policies, being limited to security assurances as discussed earlier, or provision of consumer access rights for correction purposes or the conveying of data disposal instructions.

By 2002, some policies made attempts to indicate the third parties to whom personal information would be transferred, and the level of protection provided at those destinations. Several policies attempted to address this issue, but the result was often confusion or other cause for concern – for example, "Information collected at this site may be disclosed to third parties where functions are being outsourced". The number of policies advising users how to arrange disposal of their personal information also increased to about half the policies over the two year period – as did the number of policies advising, via disclaimers, of the lack of protection of consumer personal information in other jurisdictions to which the data may be transferred.

User identification and accountability

User identification issues were poorly addressed by all policies in both years, although a few policies made (unsatisfactory) forays into these areas. Basically, a company should not adopt as a user identifier an identifier that has already been ascribed to that individual by another organisation and should state this in the policy. Also, if a consumer can use anonymous or pseudonymous identification when visiting a site, any privacy or accountability ramifications should be explained.

The policy should indicate whether a user can be held accountable for his/ her site actions through an action being indisputably linked to a user identifier. Accountability for the company includes providing for enforcement of the policy by the consumer. To support OPP quality and also consumer enforcement, privacy seals were displayed by most sites in both years. These seals provided company accountability in respect of compliance with OPP in practice, and via assuring policy quality in accordance with the seal program. Consumers could complain should they discover a privacy trustmarked site was not following its policy. Any potential accountability that could be obtained through independent audits was not reported in the policies studied.

Contact details were provided for grievance/ recourse purposes by most sites, providing a mechanism for holding companies accountable for privacy incidents or non-compliance with

policy. Few policies mentioned the consumers' responsibility to protect their own personal information in 2000, although by 2002, several policies had begun to address this issue – for example, consumers were being requested to check their data for accuracy, change their passwords from time to time, and close their browsers upon exiting the websites. However we believe it would be very difficult for users to identify their responsibilities with respect to managing their online privacy in current policies, with responsibilities currently spread throughout in piecemeal fashion.

User participation (user access, assurance, contact and choice)

An OPP should provide opportunities for user participation in online privacy protection. There was a small move toward providing greater user participation, over the two years. All sites in 2002 provided user access of some type for checking and correcting collected data, as described earlier. Users could also participate through obtaining privacy assurance via seals and certification, as mentioned earlier. The OPPs in our study did not address how the companies might incur sanctions if they failed to comply with their policies, other than to provide a contact point such as phone number or email address, where a user complaint could be lodged. Where a privacy seal is present on a site, a consumer can complain to a seal program representative about a perceived policy infringement, and the seal may be revoked if the company has indeed breached policy.

Users are sometimes contacted by companies, usually to provide a service, via contact details provided by the user. We observed that the methods available for users to opt out of such contacts were complex and discouraging, with little improvement between 2000 and 2002. Users should be given plentiful choice, particularly consent opportunities, with respect to the provision or use of their personal information. In 2000, all nine policies provided opt-out rather than opt-in for collection or use of personal information. However by 2002, most policies were offering complex combinations of opt-out and opt-in within their OPPs, which can be confusing for users. Furthermore, consent was sometimes offered covertly, for example, "By using ... and providing us with your personal information, you are accepting the privacy practices described in this policy statement". We observed a move toward offering more choices regarding information disclosed to other parties, cookies stored, subscriptions to company mailing lists, and other often unwanted services enabled by collected personal information.

Change management

As conditions change, and at regular intervals, policies should be reviewed and updated, with users being notified personally (for example, by email) that changes have been made. Other relevant changes of which users should be notified include company change of control – for example in a sale, merger or other transfer of ownership of the company. In 2000 and 2002, users were expected to keep checking the sites from time to time for policy changes, however this is a most unreasonable expectation and imposition. There was some movement by policies toward notifying users of changes via email, in 2002.

We suggest the entire area of change management for OPPs is critical to consumer trust in these policies. We recommend that companies provide users with the opportunity to be informed via email of announcements of new OPPs, and that the frequency of revised policies per annum is not overly high – no more than twice a year. Alternatively or in addition, archives of previous versions of OPPs can be stored by the company and made available to users via links placed on the site. A user can be directed to the policy version that was in place when s/he last accessed the site, and/or when s/he entered personal data; that is the policy which should apply to the data provided by the user at that time, and the policy should inform the user accordingly.

Special cases (children's privacy, sensitive information, exceptions)

Special cases including children's privacy, sensitive information and exceptions, should be articulated in the policies. Children's issues were only addressed in three OPPs in 2000, increasing to five in 2002. This is interesting because both countries studied, Australia and the U.S., require children's issues to be addressed by law. Sensitive information was

addressed in two of the policies in 2000, increasing to six in 2002. Exceptions to policies were nominated by all policies, in both years.

FINDINGS

From our study, we identified a number of significant themes. Firstly, there is a great deal of confusion for a consumer attempting to ascertain the relationship between an OPP and other online and offline company policies. Answers are needed for questions such as: "What is the relationship between an organisation's (offline) privacy policy and its OPP?" and "What is the relationship between the OPP and other online policies such as: terms of use, legal policy and security policy?" Appropriate relationships between the OPP and all kinds of other company policies must be established, so that policies can be effectively linked and integrated. At present, consumers would likely feel confounded by the loose and oft confusing linkages between these policies as currently suggested (or frequently, not suggested) by OPPs.

Taking this theme a step further, research is required to identify and/or develop links between online policies of all types, and their corresponding company offline policies. It is neither feasible nor appropriate to dump all company policies online merely by mirroring their existing offline forms, chunked into slightly smaller screen packets accessible via links from an initial list of topic headings – or worse, presented as a lengthy online document, which the user has to scroll down (tiresomely) to read in its entirety. Offline company policies were not designed to be human computer interfaces. Clearly, research into requirements for online versions of offline company policies would provide some illumination of these issues. We make a note here that a policy noticeably absent from all sites studied was an online Code of Ethics, which a site user may find useful to consult, and which could increase user trust in the company visited. Companies may well consider developing and featuring such a policy.

A second message which emerged is that there is a clear need for more usable OPPs (as was also suggested by Babu, 2000; Greenberg, 1999; Lau *et al*, 1999). Adding import to this issue, usability has been identified as an important factor in all types of online policies for the securing of consumer trust (Egger, 2001; Nielsen Norman Group, 2001). In our study, OPPs were notoriously ambiguous, difficult to read, poorly structured, and generally difficult to understand. Overall, policies were hindered by poorly designed human computer interfaces – some more so than others – and clearly would be improved by the use (during their design) of a good usability framework for OPPs. In another study, we are investigating this very issue and developing such a framework. In our work-in-progress, we are exploring the use of tools such as site maps, FAQ, summaries, audit reports and other features for improving the usability of OPPs.

A third leitmotif in this study was the lack of notice in respect of user roles and responsibilities in managing their online privacy. These important advices, when present, are typically dispersed throughout an OPP – and mostly covert, or poorly stated. In many cases, significant user roles and responsibilities (with respect to managing their online privacy) are not stated in the OPP but rather are found in other online policies, such as 'terms of use'. Relevant user roles and responsibilities must be stated explicitly within the OPP in an accessible (usable) way. For example, a user should be able to consult a single chart in the OPP, outlining all her responsibilities in managing her online privacy on a continuing basis. Clearly there is a need for researching a set of potential roles and responsibilities for the different stakeholders in managing online privacy, while appropriate techniques and human computer interface designs should be developed for presenting these duties to users in the most effective manner.

A fourth concern identified is that there is a clear need for a user to be able to consult his/her OPP history with respect to a particular site. We did not find one OPP that provided this facility, in our study – a deficiency which is bound to engender user anxiety eventually, especially once related incidents are published in the popular media with greater frequency. In a recent case involving Hotmail, many users were startled to discover they had unwittingly given their permissions – through earlier incarnations of Hotmail's OPP – for their personal information to be disclosed to third parties (Mainelli, 2002). Yet some of these users were convinced they had never given such permissions. An accurate, accessible record of the

user/ OPP history – which tracks each user's actions in respect of the OPP, including disclosure consents given and not given – would prove useful to document the facts, and make them accessible for user and company validation.

A fifth observation was that all but one of the nine OPPs studied failed to articulate the threats to a user's online privacy. eBay provided a vulnerabilities scenario analysis which provided some information in this respect. We suggest that threat analyses and vulnerability analyses are made available through the OPP, together with an outline of steps a consumer can take to minimise the vulnerability of her personal information to the threats stated. This would oblige a business to assess risks for the various online privacy threats – an exercise which would undoubtedly prove useful for the business themselves, as well as the users and indeed, other interested parties such as auditors.

A sixth emergent message was the poor linkage between online privacy policy and privacy practice, as evidenced by our case study of OzeSale, where there was apparently very little connection between the two. Normally, company policies are translated into procedures that are documented and followed, thereby facilitating not only correct implementation of the policies, but also audits and reviews. We would like to see companies developing privacy procedures from their OPPs, together with documentation of these procedures, forming some recourse for consumers with grievances.

A seventh theme was our observation of the interplay of many different types of factors in the topic area of OPP. The focus has shifted in e-Business and information systems research toward holistic approaches which integrate the human, social, organisational and technical issues (Baskerville *et al*., 2000; Lichtenstein, 2001; Lichtenstein and Swatman, 2001). We believe a comprehensive holistic framework for the development, content and factors in OPP would be of benefit to businesses. In a companion paper, we develop this idea further (Lichtenstein *et al*., 2003).

Finally, we observed through the in-depth case study some indication as to why organisations may not be following their online privacy policies in practice (indeed, such policy violations have been widely reported). It appears that privacy infrastructures within companies are not yet powerful or developed sufficiently to enforce their privacy policies inside the companies themselves, although this may be changing, with recent moves toward establishing organisational Privacy Officer functions and privacy certification with annual audits. As mentioned at the start of our paper, a study by Privacy and American Business (2002) strongly suggests that "third party verification that a company's privacy practices match its OPP" is the single most important step toward increasing consumer trust in e-Business. In an era where consumer demand for online privacy is high and the issue of trust is paramount to e-Business success, it would behoove companies to pay attention not only to improving the quality and effectiveness of their online privacy policies – but also to adhering to them, in practice.

CONCLUSIONS

We have focused in this paper on the role of effective online privacy policies in online privacy protection. We provided a set of high-level organisational guidelines for companies to use in the development of an effective OPP – as well as a descriptive analysis of the evolution of Australian and US OPPs over the past two years. Although our results are limited to a longitudinal study of nine policies over two years, and a single case study – and of course we cannot generalise from this small sample of data – our results are yet indicative of a significant improvement in the quality of OPPs over the period 2000-2002, attributed to increased public awareness of the issues combined with legislation/ industry self-regulation. One would hope to find a parallel increase in the effectiveness of OPPs and, although we have not measured this in our work, the results of the survey by Adkinson *et al*. (2002) certainly suggest this is likely. Nonetheless, we identified a significant shortfall between policies, and the requirements for such policies as indicated by our guidelines. We suggest that business use of our guidelines would improve OPPs substantially, as well as adding to existing empirically-based theory in this area (theory of which there is little to date).

Our guidelines are preliminary, in that they are based on the small sample of data explored, and are therefore highly unlikely to yield all of the issues or requirements for OPP guidelines.

However, we believe we have provided a solid foundation upon which to build, in future research. Combining our interpretive analysis approach with the quantitative content-based approach of Anton and Earp (2001) may yield interesting results, as may a combination of that approach with other forms of empirical research – for example, a focus group comprised of representatives from key stakeholder groups.

In conclusion, we comment on the future importance of privacy research in the e-Business domain. With trends in e-Business waxing and waning, and experts in disagreement about the importance of any single e-Business issue to eventual success, online privacy has shown remarkable consistency in retaining its position in the paramount online consumer concerns, since the earliest days of the Internet – just as privacy in general has remained important to humans since the earliest days of mankind. In times of lessening certainty about our personal safety, and consequent increasing threats to our privacy, we believe that making an effort to protect and assure personal privacy is of greater importance now than ever before, and urge e-Business researchers not to lose sight of this highly-prized, human right – as Warren and Brandeis put it over one hundred years ago in 1890, "the right to be let alone".

REFERENCES

Adkinson, W.F. Jr., Eisenach, J.A. and Lenard, T.M. (2002) *Privacy Online*: *A Report on the Information Practices and Policies of Commercial Web Sites*, Progress & Freedom Foundation, March, Washington, DC.

Agre, P.E. and Rotenberg, M. (1997) *Technology and Privacy*: *the New Landscape*, MIT Press.

Anderson (2001) *Anderson Legal/Arthur Anderson Internet Privacy Survey 2001.* Anderson Legal/Anderson Worldwide, Melbourne, Australia.

Anton, A.I. and Earp, J.P. (2001) *A Taxonomy for Web Site Privacy Requirements*. NCSU Dept. of Comp Science Technical Report, TR-2001-14.

APCC (2001) *The Australian Privacy Seal Audit and Certification Program*, Australian Privacy Compliance Centre, West Perth, Australia.

Babu, K. (2000) *Effective Privacy Assurance for E-Commerce Web Sites*. unpublished Honours Thesis, available from Library of School of Information Management and Systems, Monash University, Melbourne, Australia.

Baskerville, R., Stage, J. and DeGross, J. (Eds.) (2000) *Organization and Social Perspectives on Information Technology*. Kluwer Academic Publishers, Boston.

Bingi, P., Mir, A. and Khamalah, J. (2000) The Challenges Facing Global E-Commerce. *Information Systems Management*, Fall.

Chung, W. and Paynter, J. (2002) Privacy Issues on the Internet. In *Proceedings of the 35th Hawaii International Conference on System Sciences*, Sprague, R.H. and Nunamaker, J.F. (Eds.), Hawaii, IEEE Computer Society Press, Los Alamitos, California.

Clarke, R. (1999) *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*. Xamax Consultancy Pty Ltd., http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html

Cranor, L.F., Reagle, J., Ackerman, L.S. (2000) Beyond Concern: Understanding Net Users' Attitudes About Online Privacy. In Vogelsang, I. and Compaine, B.M. (Eds.) *The Internet Upheaval*: *Raising Questions, Seeking Answers in Communications Policy*. Cambridge, Massachusetts: The MIT Press.

Culnan, M.J. (1999) *Georgetown Internet Privacy Policy Survey*: *Report to the Federal Trade Commission*. June. http://www.msb.georgetown.edu/faculty/culnanm/GIPPS/gipps1.PDF

Egger, F.N. (2001) Affective Design of E-Commerce User Interfaces: How to Maximise Perceived Trustworthiness. In: Helander, M., Khalid, H.M. and Tham (Eds.), *Proceedings of CAHD2001*: *Conference on Affective Human Factors Design,* Singapore, June 27-29, 2001: 317-324.

enonymous (2000**)** *Internet Privacy*: *a summary of privacy ratings research by enonymous.com.* http://interviewing.com/enon/

EPIC (1999) Report Slams Privacy Policies; Poll Finds Privacy is Top Concern. *Epic Alert*, Vol. 5, No. 15.

FTC (2000) *Privacy Online*: *Fair Information Practices in the Electronic Marketplace*: *A Federal Trade Commission Report to Congress*. Federal Trade Commission, US.

Freehills (2000) *Internet Privacy Survey*. Freehills Law firm, Melbourne, Australia.

Greenberg, I. (1999) Facing Up to New Interfaces. *Computer*, IEEE, April, Vol. 32, No. 4, pp 14-16.

Harvey, J.A. and Sanzaro, K.M. (2002) *P3P and IE 6*: *Raising More Privacy Issues Than They Resolve?* Gigalaw.com, February, http://www.gigalaw.com/articles/2002-all/harvey-2002-02-all.html

Hoffman, D.L., Novak, T.P. and Peralta, M. (1999) Building Consumer Trust Online. *Communications of the ACM*, Vol. 42, No. 4, April.

Lau, T., Etzioni, O. and Weld, D.S. (1999) Privacy Interfaces for Information Management. *Communications of the ACM.* Vol. 42, No. 10, pp 88-94.

Lichtenstein, S. (2001) *Internet security policy for organisations*. PhD thesis (public version), School of Information Management and Systems, Monash University, Melbourne, Australia.

Lichtenstein, S. and Swatman, P.M.C. (2001) Effective Management and Policy in E-Business Security. *Fourteenth International Bled Electronic Commerce Conference,* Bled, Slovenia.

Lichtenstein, S., Swatman, P.M.C., and Babu, K. (2003) Adding Value to Online Privacy for Consumers: Remedying Deficiencies in Online Privacy Policies With an Holistic Approach. *36th Hawaii International Conference on System Sciences HICSS-36*, January 6-9, 2003, Hawaii, USA.

Mainelli, T. (2002) Hotmail Policy Raises Privacy Concerns. *PCWorld.com*, May 27.

Nielsen Norman Group (2001*) E-commerce User Experience*: *Design Guidelines for Trust and Credibility*. Nielsen Norman Group. http://www.nngroup.com/reports/ecommerce/trust.html

NPP (2000) *National Privacy Principles*. Office of the Federal Privacy Commissioner, Canberra, Australia.

OECD (1980) *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data*, OECD, Paris, France.

OPA (2002) *Guidelines for Online Privacy Policies*, Online Privacy Alliance, Washington, DC.

Privacy & American Business (2002) *Privacy On and Off the Internet*: *What Consumers Want*. Privacy & American Business, Hackensack, NJ.

Reagle, J. and Cranor, L.F. (1999) The Platform for Privacy Preferences. *Communications of the ACM*, *Vol. 42, No.2.* pp 48-55.

Richmond, M. (1999) *A Framework of Guidelines for the Development of Internet Privacy Policy*, unpublished Honours Thesis, available from Library of School of Information Management and Systems, Monash University, Melbourne, Australia.

Warren, S. and Brandeis, L. (1890) The Right to Privacy. *Harvard Law Review*, Vol. IV, No. 5, December 15.

Westin, A. (2001) *Opinion Surveys*: *What Consumers Have to Say About Information Privacy*. Executive Summary, Prepared Witness Testimony, The House Committee on Energy and Commerce, US. Available: http://energycommerce.house.gov/107/hearings/05082001Hearing209/print.htm

W3C (2002) *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*: *W3C Recommendation 16 April 2002*. World Wide Web Consortium, MIT, MA.

ACKNOWLEDGEMENTS

The authors wish to thank the three anonymous reviewers for their helpful comments about an earlier version of this paper.

COPYRIGHT