This is the published version:


Available from Deakin Research Online:

http://hdl.handle.net/10536/DRO/DU:30005148

Reproduced with the kind permissions of the copyright owner.

Copyright : 2003, ECIW
TRENDS AND GUIDELINES IN ONLINE PRIVACY POLICY

Shirman Lichtenstein1, Paula M C SWATMAN2 and Kanchan Babu3

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

2Faculty of Informatics, University of Koblenz, Koblenz, Germany, and School of Information Systems, Deakin University, Melbourne, Australia
paula.swatman@uni-koblenz.de

3Telstra Retail, Melbourne, Australia
anitha.babu@team.telstra.com

ABSTRACT

Online privacy policies (OPP) are important mechanisms for informing online consumers about the level of information privacy protection afforded when visiting web sites. To date, societal mechanisms and technologies have been the focus of attempts to improve the quality and effectiveness of OPPs. We present findings from a longitudinal, empirical study of online privacy policies. Our research found that although online privacy policies have improved in quality and effectiveness since 2000, they still fall well short of the level of privacy assurance desired by consumers. This study analyses trends in OPPs over the two years of the study, identifying areas of deficiency and improvements, and offering a solution in the form of a detailed set of guidelines for organisational online privacy policy. Our study adds to existing theory in this area and, more immediately, will assist businesses concerned about the effect of privacy issues on consumer web usage.
1. INTRODUCTION

The importance of information privacy to e-business has been recognised for some time (Agre and Rotenberg, 1997), with the Gartner Group nominating information privacy as the greatest single obstacle to consumer-based e-business up to 2006 (Zero-Knowledge Systems, 2003). Information privacy addresses the legitimate collection, use and disclosure of personal information (PI), as well as "the claims of individuals that data about themselves should generally not be available to other individuals and organisations, and that, where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use" (Clarke, 1999).

Set against a backdrop of public distrust of institutions, fears of technology abuse, a relentless stream of privacy incidents, and governmental reaction to terrorism resulting in calls for personal accountability and PI aggregation (see current US plans for a Total Information Awareness (TIA) program), information privacy issues are also very much at the forefront of public thinking. In the post September 11 industrial world, many people are understandably fearful of criminal Internet activity, anticipating changes in the ways companies handle privacy issues in future (PAB, 2002a; BIP, 2002).

The consumer concerns in online privacy (Cranor et al., 2000; Wang et al., 1998) centre 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). In another study, key consumer privacy issues were identified as the sale, theft, loss or destruction of PI, and spam (Dhillon & Moores, 2001). In response to the privacy threat, consumers often take steps to reduce these perceived risks, including entering false personal information into web sites (Fox et al., 2000; Gellman, 2002).

Not surprisingly, organisational efforts to address consumer privacy issues reflect strategies intended both to gain consumer trust and loyalty, as well as establish a competitive differentiator (Deloitte Research, 2002; Hoffman et al., 1999; PAB, 2002c; Schoder & Yin, 2000; Westin, 2001). Considerable pressure has also been brought to bear by government upon businesses to attend to corporate governance and ethics following the Enron and Worldcom scandals, with increased attention filtering through to the privacy issues. Other incentives for companies to respond to consumer privacy concerns include fears of unfavourable media publicity and litigation in the event of privacy breaches, particularly given the recent enactment of privacy regulation in many jurisdictions. In summary, while companies wish to maximise their leverage from PI, they also have a vested interest in providing adequate privacy protection — and accordingly, a variety of organisational solutions have been developed for this purpose, with a potentially powerful member of this group of approaches being the online privacy policy (OPP).

The OPP, or privacy statement, is viewed as a key organisational tool for providing online privacy protection (Agranoff, 1993; Chung & Paynter, 2002). These policies articulate the manner in which a company collects, uses and protects data, and the choices offered to consumers for exercising their rights in respect of the use of their own personal information (Babu, 2000). OPPs are intended to reflect fair information privacy principles, as originally defined by OECD (1980), and subsequently extended and modified by different countries to accommodate perceived e-business and globalisation needs (for example, NPP, 2000). Consumers are able to access OPPs (if available) when visiting sites, thereby obtaining understanding of the company's privacy policy, practices and procedures — and becoming better equipped to make informed choices regarding engaging with the business or providing consent to PI collection, use or disclosure.

Recently, surveys have highlighted the importance of effective, quality OPPs for companies wishing to gain online consumer trust and, in turn, consumer business (Columbus Group and Ipsos-Reid, 2001; PAB, 2002c). To date, however, OPPs have rated poorly in this regard, possessing a rather less than perfect record in effecting privacy protection (FTC, 2000; Freehills, 2000; PAB, 2002c), Watt et al.
(2002) found that Australian OPPs in September 2001 did not yet satisfy recognised sets of fair information privacy principles, despite recent regulation. Earlier, in 2000, we had pondered a similar concern about the inadequacies of existing OPPs, feeling that the existence of fair information practice principles – together with impending regulation – would not be sufficient to guide organisations in developing these policies. We believed that more comprehensive guidance was needed by companies attempting to develop effective OPPs, and in early 2000, we commenced a study with this objective (reported in Babu, 2000). Two years later, we repeated our study in order to obtain a picture of trends in OPP, especially considering changes in the regulatory and awareness scenes which had taken place in that time.

In other work, we have provided a broad discussion of deficiencies in OPP, a high-level set of organisational guidelines for OPP; and an holistic approach to developing OPPs (Lichtenstein et al., 2002; 2003). In this paper, we provide an in-depth comparison of OPPs in 2000 and 2002 obtained from a longitudinal study of OPPs undertaken in 2000 and 2002 – as well as a comprehensive, detailed set of organisational guidelines for OPP.

Our aim in this paper is to investigate the potential for a set of organisational guidelines for the development of effective OPP. The remainder of this paper is structured as follows. In Section 2, we overview our research methodology. In Section 3, we discuss the role of OPP in online privacy protection. Section 4 provides a detailed set of organisational guidelines for effective OPP, together with an in-depth comparison of OPPs in 2000 and 2002, highlighting trends. Finally, we draw conclusions, and posit future research directions.

2. METHODOLOGY

The approach used was a longitudinal study, conducted in 2000 and 2002. Babu (2000) commenced the study by compiling a first-cut model of organisational guidelines for OPP, consisting of important privacy principles suggested in the literature integrated with all principles discovered in existing sets of fair information privacy principles. Babu then investigated OPPs at web sites of eight American businesses and two Australian businesses, using the guidelines to guide the study. The sites (ebay.com, cdnow.com, 247realmedia.com, colesonline.com.au, wishlist.com.au, travel.com, disney.com, toymart.com, craftshop.com, and realnetworks.com) were selected because they were highly active, well-recognised e-business sites at the time of study, and because they featured substantial OPPs. This group of sites included five retail organisations, one auction service, one travel site and three entertainment companies.

First, the OPPs were evaluated for compliance with the first-cut guidelines in order to identify deficiencies in the policies. Guideline compliance was measured by its reasonable implementation within a policy. Second, a content analysis of the OPPs was performed as a strategy for discovering unexpected, novel and useful elements which could be incorporated in future editions of the guidelines. Third, the policies were analysed contextually, evaluating the influence of HCI, organisational and human factors on the perceived effectiveness of the policies, thus identifying new elements for future editions of the guidelines, as well as providing further evidence of policy weaknesses. A cross-policy analysis comparing the policy evaluations elicited trends, patterns and differences, highlighting the levels of weakness in different aspects of OPP at that time. All newly identified elements from the investigation were added to the first-cut guidelines, resulting in a revised set of guidelines for OPP, and completing the component of the research project undertaken in 2000.

In the second stage of this project – our extension in 2002 of the original investigations from 2000 – we first reviewed the earlier research from 2000. We then analysed the nine still-existing OPPs in their updated forms in 2002, using the same methods as in 2000 – evaluation of policies for deficiencies, content analysis, contextual analysis and cross-policy analysis. In this way, we arrived at a number of interesting results and findings – including a detailed set of organisational guidelines for OPP, and a comparison of policies in 2000 with their 2002 equivalents, indicating trends in OPP over this period.
3. THE ROLE OF THE ONLINE PRIVACY POLICY IN ONLINE PROTECTION

3.1 Performance of OPP

How have OPPs fared in practice, to date? Recent studies revealed that significant proportions of US and Australian OPPs failed to comply with recognised fair information practice principles and, overall, were ineffective (Anton and Earp, 2001; Babu, 2000; Culnan, 1999; EPIC, 1999; FTC, 2000; Freehills, 2000; PAB, 2002c). These studies found that OPPs, terms of service, conditions of use and other online policies were frequently overlooked by users in their eagerness to gain access to online products and services. Typically, users either signaled consent to policy conditions without reading the policies, or declined them unread. Policies were frequently unclear – for example, they were ambiguous, couched in “legalese”, misleading or deceptive. More disturbingly, OPPs were found to be inconsistent with actual privacy practices, and poorly linked to business strategy and operations in general.

Encouragingly, there have been recent reports of improvement in Australian and American policy quality and prevalence, possibly due to various levels of regulation and/or increased media attention given to the issues (Adkinson et al., 2002; Anderson, 2001; Watt et al., 2002). Freehills (2000) reported that only 12% of Australian commercial sites in 1999 featured an OPP – but according to Watt et al. (2002), by September, 2001 - a date shortly before the federal government-set privacy law compliance deadline of December that year – the estimated incidence had risen to 64%. Despite all these positive signs, however, reports continue to observe the role of ineffective OPPs in the seemingly unending stream of online privacy incidents (for example, Mainelli, 2002).

3.2 Support for OPPs

There are a variety of approaches to societal and technological support for OPPs. The European Union (EU) established fairly stringent privacy legislation some years ago (EU, 1998), in the process setting strict privacy requirements for other countries which wished to do business with EU nations. In Australia, co-regulation is a recent approach to the problem (NPP, 2000) while in the US, industry self-regulation holds sway (FTC, 2000), although future legislation appears likely (see, for example, Hollings, 2002). Canada has elected to follow the EU example, albeit more narrowly (Canadian DOJ, 2001). 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).

In terms of technological support, a landmark development has been P3P, which enables consumers to view a translated version of a site’s OPP in more usable form, and facilitates comparisons of consumer privacy preferences with policy privacy levels (W3C, 2002). However, critics have debated the effectiveness (and pointed out the limitations) of this approach and observe that, to date, few companies have adopted this technology (Harvey and Sanzaro, 2002). Of note, there has been a recent emergence of privacy management technologies (Hunt, 2003), although it is still too soon to evaluate their effectiveness, or even their potential.

3.3 Need for organisational guidance in OPPs

Firms can also employ organisational methods for guiding the development and support of their OPPs. However, we believe existing sets of “organisational guidelines” are inappropriate for this purpose. The majority of current guidelines are, fundamentally, national fair information practice principles (for example, NPP, 2000), and were developed purely on the basis of professional expertise, rather than being founded on rigorous research methods. These guidelines may therefore have missed some of the issues.
Some progress has been made in developing empirically grounded organisational guidelines. 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, the ongoing (and frequent) occurrences of online privacy incidents suggests that existing OPPs are ineffective in managing the risks, and do not reflect privacy practice — both because of deficiencies in current sets of guidelines, as well as lack of integration of OPPs with practice. This project has resulted in a set of extended organisational guidelines for OPPs, as we now discuss.

4. TRENDS AND ORGANISATIONAL GUIDELINES FOR OPP

In this section, we provide a comprehensive set of high-level guidelines for online privacy policies, covering the following fourteen categories: awareness, data quality, choice, security, information movement, user participation, assurance, children's privacy, change, user identification, sensitive information, accountability, contact and exceptions (compiled from Babu, 2000; Anton and Earp, 2001; NPP, 2000; FTC, 2000 and our own empirical studies). For presentation and comprehension, we have grouped the guidelines into seven tables representing the following OPP areas: awareness, data quality and security, information movement, user identification and accountability, user participation, change and special cases. Note 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. Our set of guidelines is intended as a map for businesses, to ensure that all important areas are addressed in the development of OPPs.

Overall, we found that the OPPs studied in 2002 had improved in quality since 2000. We attribute this development mainly to an increased consciousness of online privacy issues within the e-business community, combined with privacy legislation or industry self-regulation founded upon recognised fair information practice principles. Despite our finding of overall quality improvement since 2000, we nevertheless found that a significant portion of the guidelines in our set were still inadequately addressed or missing from many of the OPPs. In the remainder of this section we discuss trends and issues arising from our study of the nine policies. In the interests of limiting the paper’s size, we have restricted discussions to selected aspects from each table.

<table>
<thead>
<tr>
<th>Awareness Guidelines</th>
<th>Brief Description of Guideline</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Awareness</strong></td>
<td>The company should facilitate user awareness of its privacy policies.</td>
</tr>
<tr>
<td>1.1 Prominence/openness</td>
<td>A clearly-labelled link to the policy should be displayed in a conspicuous manner and position on every page. The company should provide the company's privacy policy and relevant explanations to a user, on request.</td>
</tr>
<tr>
<td>1.2 Language</td>
<td>The policy should be written in simple English, and be clear, logically-structured, consistent and unambiguous.</td>
</tr>
<tr>
<td>1.3 Notification</td>
<td>The policy link should be made available whenever personal information is requested by the web site—in a prominent position, adjacent to the data collection boxes.</td>
</tr>
<tr>
<td>1.4 Classification</td>
<td>The policy should identify each field of personal information collected by the site.</td>
</tr>
<tr>
<td>1.5 Collection</td>
<td>Personal information collected should be linked to the transaction that the user is engaged in at the time of providing it.</td>
</tr>
<tr>
<td>1.6 Purpose/use</td>
<td>Personal information collected should only be disclosed or used for purposes related to the original collection purpose.</td>
</tr>
<tr>
<td>1.7 Disclosure</td>
<td>Sites should state third parties to whom information will be disclosed, and exactly which information will be disclosed to each party, with conditions of disclosure clearly stated.</td>
</tr>
<tr>
<td>1.8 Consumer education</td>
<td>The site should provide, or link to, consumer education about online privacy issues, rights and responsibilities.</td>
</tr>
<tr>
<td>1.9 Third party involvement</td>
<td>The user should be informed about company or user responsibilities with respect to online privacy protection at third party sites linked to by the site, or by other third parties to which information may be disclosed.</td>
</tr>
</tbody>
</table>

Table 1: Awareness guidelines for online privacy policy
4.1 Awareness (Table 1)

A company has a duty to promote user awareness of the online privacy issues resulting from a site visit. The minimum requirement is a conspicuous link to the OPP, located in a consistent location on each page of the site—and, indeed, we found that all the nine sites studied featured such a link in both 2000 and 2002 (although many quite sizeable companies either have no OPP at all, or locate it somewhere on the web site where visitors must search hard to find it). The next level of facilitating user awareness is to provide a conspicuous link to the OPP whenever user privacy is being threatened in some way, for example when personal information is being requested from a user. None of the sites provided this type of awareness in 2000, although a few did in 2002 in respect of data collection and several other privacy threats.

With respect to communication quality, which is clearly required for effective user awareness, most sites were still written in moderately complex English, in both 2000 and 2002. We also found many misspellings, inconsistencies, legalese, and other confusing aspects of expression and layout—making most policies difficult to comprehend or navigate.

Another aspect of awareness is a clear explanation of the level of detail of the personal information being collected by the site. Most sites, in both 2000 and 2002, failed to provide this level of detail. As an example of the 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...". By contrast, eBay featured a very informative, complete, personal information access chart, with each field of personal information plotted against those third parties granted the specified accesses, once the information had been collected by the site.

Other types of awareness are also needed. An OPP should make the user aware of the purpose for which personal information is being collected. We found minimal linking of collected personal information to individual user transaction purpose in both years, although sites did provide general reasons for collecting personal information overall—for example, "We use that information to service your account and to personalize your experience at...", and several sites provided long lists of specific uses, although each of the items listed was still fairly general.

Informing the user of potential future disclosure of their information is a further important component of awareness. We found considerable complexity in the way such disclosure information was presented, with little information about the conditions under which disclosures would take place. Confounding the user about disclosure practices was common. 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 e-mailing the user—for example, placing pop-up advertisements on the user's computer.

Consumer education intended to increase user awareness of online privacy issues was missing from all policies in 2000, with the exception of a single OPP which provided links to recognised information privacy expertise sites. By 2002, however, four of the OPPs provided such links. Despite these signs of improvement, we believe that much more than links to expert sites is needed for effective consumer education.

Another company responsibility is to inform users about the level of protection afforded by third parties to which the site links, as well as by other third parties with which personal information could be shared in the future. In 2000, only three policies provided privacy protection information about third party sites linked to (and these were merely disclaimers), increasing to eight in 2002 (mostly disclaimers, although some were assurances of similar levels of privacy protection). Hence, there has been some improvement in this area.
4.2 Data quality and security (Table 2)

Six OPPs facilitated user access for the purpose of checking and correcting collected personal information, increasing to nine in 2002. In many cases the user was given, as the only access method, a contact email address rather than a form to use when updating information, making it considerably more difficult for users to correct errors.

With respect to the security of online data, there are two quite separate issues which need to be addressed. Firstly, companies need to ensure they provide adequate protection during the updating of information and, consequently, during the transfer of data over the Internet. This is the issue which concerns the majority of website users, who are often not aware that the danger of loss or compromised data in transit is actually a comparatively minor issue. Secondly, and probably even more importantly, companies must be certain that they have fully protected their stored PI from unauthorised access, damage to integrity, and unauthorised destruction. This issue is often completely unconsidered by consumers, but is the greatest data risk for anyone who deals with companies today (even those who do not take orders over the Internet, since any company with Internet access is also vulnerable to attack through that very access point (CSI, 2002; Gibbs et al., 2002)).

In all situations, total responsibility for data quality assurance rested with the user, with none being guaranteed by the company (other than security assurances) as follows. Five OPPs in 2000, increasing to all firms in 2002, provided some commitment to data security, indicating use of SSL, firewalls and other technologies, with corresponding symbols such as padlocks on the sites. General security assurance statements were commonly found, for example, ‘We employ many different security techniques to protect such data from unauthorized access by users inside and outside the company’, while general disclaimers were popular, for example, ‘...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’. By 2002, however, two of the OPPs listed extensive security provisions, while other sites had improved and added to theirs. For example, one OPP assured: secure connections from customer browser to company site, encryption for sensitive personal information, logical security of company databases, access controls to such databases, and employee data-confidentiality contracts. We view this as a promising trend.

In 2000, none of the policies provided information about the security of data in transmission (for example, the risk that it could be intercepted in transmission), although by 2002 almost all policies were providing disclaimers about information protection while in transmission.

4.3 Information movement (Table 3)

A few sites in 2000, and all sites in 2002, made some commitment to explaining their use of cookies as a form of monitoring or tracking for the purpose of better serving the user. Although the level of detail provided was sometimes quite high, it was still too easy to miss the import of a monitoring use when buried amongst wordy explanations.
Aggregation of information within OPPS was often inconsistent. For example, one policy stated in one section that anonymous (that is, non-personally identifiable information (PII), such as IP address) information would not be linked to the user’s PII without his/her consent (that is, there was choice) while, in another section, the policy stated that it would in future be considering giving the user a choice as to whether the anonymous information collected could be linked to PII, as currently the information could be linked (that is, there was no user choice). Regarding information storage, only data quality or security issues were addressed in policies (as discussed earlier), and the duration of storage was not made explicit in most cases, in either year.

Policies made limited attempts to indicate where personal information would be transferred, as was discussed earlier. Information disposal was another area with little consistency or care shown. In 2002, four of the policies referred to the user needing to take responsibility for deleting their own personal information via email, and/or mentioned that personal information would be deleted once the user had completed a related transaction (for example, an email enquiry). The other five policies did not address the issue of information disposal. Information personalisation was addressed by all policies in a very general manner in 2002, with statements such as ‘information collected is used to provide the customer with better service’. Information protection - should collected personal information cross borders - was addressed by about half the policies in 2002.

### Table 3: Information movement guidelines for online privacy policy

<table>
<thead>
<tr>
<th>Information Movement Guidelines</th>
<th>Brief Description of Guideline</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Information Movement</td>
<td>Information privacy protection should be provided in all states of information movement.</td>
</tr>
<tr>
<td>4.1 Information monitoring</td>
<td>Policies should specify and explain monitoring of user activity through cookies, etc.</td>
</tr>
<tr>
<td>4.2 Information aggregation</td>
<td>Policies should inform users about use of aggregation of personal information with data from other sources, and any linking of aggregated data with other data, in particular, PII.</td>
</tr>
<tr>
<td>4.3 Information storage</td>
<td>Policies should inform users about personal information stored in the company systems, as well as the purpose and duration for which the information is stored.</td>
</tr>
<tr>
<td>4.4 Information transfer</td>
<td>Policies must state to whom, why and when collected personal information will be transferred, as well as other relevant conditions.</td>
</tr>
<tr>
<td>4.5 Information disposal</td>
<td>Policies should inform users of how and when they dispose of personal information. This should be when the purpose for which the information was collected has been completed.</td>
</tr>
<tr>
<td>4.6 Information personalisation</td>
<td>Policy should state how the site plans to personalise services offered to them by using personal information collected from the user.</td>
</tr>
<tr>
<td>4.7 Transborder data flow</td>
<td>Privacy assurance afforded when information crosses borders, should be addressed.</td>
</tr>
</tbody>
</table>

### Table 4: User identification and accountability guidelines for online privacy policy

<table>
<thead>
<tr>
<th>User identification and accountability guidelines</th>
<th>Brief Description of Guideline</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. User Identification</td>
<td>The use and disclosure of a user’s site identifier as either PII, anonymous, or pseudonymous, should be addressed.</td>
</tr>
<tr>
<td>5.1 User identifier</td>
<td>The company should not adopt as the user identifier, an identifier ascribed to that individual by another organisation.</td>
</tr>
<tr>
<td>5.2 Anonymity</td>
<td>If a user can employ anonymous identification, the ramifications for the user should be explained.</td>
</tr>
<tr>
<td>5.3 Pseudonymity</td>
<td>If a user can employ pseudonymous identification, while still being held accountable, the ramifications for the user should be explained.</td>
</tr>
<tr>
<td>5.4 Nonrepudiation</td>
<td>The policy should indicate whether a user can be held accountable for his/her site actions through action being indisputably linked to a user identifier.</td>
</tr>
<tr>
<td>6. Accountability</td>
<td>Company and user should each be held accountable for their actions with respect to online privacy.</td>
</tr>
<tr>
<td>6.1 Enforcement</td>
<td>There should be a mechanism by which the user can enforce the policy.</td>
</tr>
<tr>
<td>6.2 User responsibilities</td>
<td>User responsibilities in safeguarding their online privacy should be explained.</td>
</tr>
</tbody>
</table>
4.4 User identification and accountability (Table 4)

User identification issues were poorly addressed by policies in both 2000 and 2002. A few policies made forays into these areas, but we do not believe the explanations provided would be comprehensible to the average Internet user. With respect to accountability, the only mechanisms for user enforcement of policy provided by most OPPs in both years was an email contact address, and/or the presence of privacy seals. Five sites in 2000 and seven in 2002 bore a privacy seal (for example, TRUSTe), while email address contacts were provided in almost all cases in both years. One site discouraged all contact, claiming it did not have the resources to respond to enquiries and that the user would be kept waiting if they enquired.

Very little information about user roles and responsibilities featured in the policies. Some small attempts at this have been made in the policies reviewed over the two year period, indicating that companies are now more aware of this important aspect of OPPs. In some policies, users were advised to safeguard their passwords, and to sign off and close browsers at the end of accessing the sites, but this was not made compulsory in any of the sites. Finally, we believe it would be very difficult for users to identify their responsibilities for managing their online privacy from existing policies, since these responsibilities are currently spread throughout the documents in piecemeal fashion.

4.5 User participation (Table 5)

An OPP should provide opportunities for user participation in their own privacy protection. All sites in 2002 provided user access to their own personal information via either an online form or via email contact, in order to check and correct their information. Some policies addressed situations in which users were given access to other users' personal information through the web site's facilities, for example via bulletin boards where users could post notices including their email addresses, names and so forth.

Users can also participate through obtaining (re)assurance. In order to provide verification that a company is adhering to its OPP in practice, the company can seek certification (via annual audit) and display a corresponding seal – such as the Australian Privacy Seal (APCC, 2001). The presence of such a seal on the site “provides potential customers with a sense of assurance that a site’s policies and business practices are legitimate and trustworthy” (Sciortino, 2002). Five sites in 2000 and seven in 2002 bore a privacy seal such as TRUSTe.

Statements of guarantee in the policy can also reassure the user. We found that some companies had loopholes in these. For example, RealNetworks in 2002 stated it would use ‘reasonable efforts to comply with this privacy policy and will take prompt corrective action when it learns of any failure to comply with our privacy policy’ but indicated that it frequently released early versions (alpha and beta) of its products which, being merely test products, could quite possibly result in unintended privacy issues.

The OPPs in our study did not address how the companies would 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 seal is present on the site – for example, the Australian Privacy Seal – the consumer can complain to a representative of that organisation about a perceived policy infringement, and the seal can be revoked if the company has indeed breached policy. What the impact of such revocation would be, however, is unclear. Indeed, there is a growing body of literature which suggests that users take very little notice of privacy seals within web sites. For example, Cranor et al. (2000) noted that: “while a large number of respondents said they would be more likely to provide information in a scenario where a Web site had a privacy policy and a seal of approval, privacy seals were among the least important criteria for determining whether or not to provide information to Web sites”.

91
Users are sometimes contacted by companies 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.

<table>
<thead>
<tr>
<th>User participation guidelines</th>
<th>Brief Description of Guideline</th>
</tr>
</thead>
<tbody>
<tr>
<td>7. User Access</td>
<td>Users should have opportunity to participate in their personal information protection as necessary.</td>
</tr>
<tr>
<td>7.1 User access and correction, to own data</td>
<td>Companies should allow users to have fair and suitable access to their own information. When necessary, the user should be allowed to modify or add to the data held about him/her, and if legally justified, the user should be allowed to erase the data.</td>
</tr>
<tr>
<td>7.2 User access to other users’ data</td>
<td>Policies should state any privacy protection for user access to other users’ data.</td>
</tr>
<tr>
<td>8. Assurance</td>
<td>Policies should state ways in which companies assure users that they are following OPPs in practice.</td>
</tr>
<tr>
<td>8.1 User recourse</td>
<td>A company should provide users with mechanisms by which their complaints can be resolved, for example, a company Privacy Officer’s e-mail address.</td>
</tr>
<tr>
<td>8.2 Verification</td>
<td>There should be a mechanism by which the company’s privacy practices can be verified by the user—for example, a privacy seal.</td>
</tr>
<tr>
<td>8.3 Consequences</td>
<td>There should be procedures in place which deal with companies which fail to comply their OPPs.</td>
</tr>
<tr>
<td>9. Contact</td>
<td>Policies should state how, and for what purpose, organisations contact users, using PII to make the contact. Users should have an opportunity to opt-out of contact.</td>
</tr>
<tr>
<td>10. Choice</td>
<td>The user should be given choices with respect to collection and use of personal data.</td>
</tr>
<tr>
<td>10. Consent</td>
<td>The web site should offer users the option to opt-out or opt-in of personal data collection, disclosure to other parties, and services provided based on personal information collected.</td>
</tr>
</tbody>
</table>

Table 5: User participation guidelines for online privacy policy

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. By 2002, however, most of the 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 the collection of personal information.

<table>
<thead>
<tr>
<th>Change management guidelines</th>
<th>Brief Description of Guideline</th>
</tr>
</thead>
<tbody>
<tr>
<td>11. Change management</td>
<td>Companies require procedures for change management of their OPPs.</td>
</tr>
<tr>
<td>11.1 Evolution</td>
<td>The company should conduct regular reviews of the company privacy practices and privacy policies. The privacy policy should include changes that have occurred in regard to the handling of personal information.</td>
</tr>
<tr>
<td>11.2 Changes to policy</td>
<td>A company should inform its customers whose material it has collected of material changes in its information privacy practices.</td>
</tr>
<tr>
<td>11.3 Change of company control</td>
<td>A company should inform users about personal information protection in the event of a sale, merger, or other transfer of ownership of the company.</td>
</tr>
</tbody>
</table>

Table 6: Change management guidelines for online privacy policy

4.6 Change management (Table 6)

In 2002, mention was made in several policies that there would be policy reviews, and hence changes, in policy from time to time. Some sites announced these changes in advance, giving ‘fair warning’. In most of the OPPs evaluated in 2002, the user is advised to check back at the site ‘from time to time’ to see if a new version of the OPP existed. It is unreasonable to expect a user to recall the version of the
policy which was in place during previous site accesses, especially as those accesses may be sporadic and/or spaced well apart in time.

We suggest 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 should not be too high. Alternatively, or perhaps in addition, archives of previous versions of OPPs could be stored by the company and made available to users via links placed on the site. A user could then be directed to the policy version which was in place when s/he last accessed the site, and/or when s/he entered personal data; that is the policy version which should apply to the data provided by the user at that time, and the policy should inform the user accordingly. In 2000, only two of the policies advised users of the impact of a change of company control on user information privacy, although in 2002 five of the policies mentioned this.

<table>
<thead>
<tr>
<th>Special Cases Guidelines</th>
<th>Brief Description of Guideline</th>
</tr>
</thead>
<tbody>
<tr>
<td>12. Children’s Privacy</td>
<td>The policy should dictate clearly regarding the involvement of children. The policy should state whether minors are permitted to use the site and the parental consent that is required, if they are so permitted. Parental consent should be verifiable.</td>
</tr>
<tr>
<td>13. Sensitive information</td>
<td>Sensitive information should be treated differently to other personal information, for example, religious beliefs.</td>
</tr>
<tr>
<td>14. Exceptions</td>
<td>Exceptions to the policy should be clearly stated.</td>
</tr>
</tbody>
</table>

Table 7: Special cases guidelines for online privacy policy

4.7 Special cases (Table 7)

Children’s privacy issues were addressed in only three OPPs in 2000, increasing to five in 2002. This is interesting because both of the countries studied - Australia and the US - 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 were nominated by all policies in both years.

5. CONCLUSION

We have focused in this paper on the role of effective online privacy policies in online privacy protection. We provided both a detailed set of organisational guidelines for companies to use in the development of an effective OPP and a descriptive analysis of the evolution of Australian and US OPPs between the period 2000-2002. Although our results are limited to a longitudinal study of nine policies over two years – and of course we cannot generalise from this small sample of data – our results are nonetheless indicative of a significant improvement in the quality of OPPs over the period 2000-2002, which could well be 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, results of the survey by Adkinson et al. (2002) certainly suggest that this is likely.

Despite the undoubted improvements in OPP over the two years, however, we also found a significant shortfall between extant policies and the requirements suggested by our guidelines. Clearly, more work needs to be done in improving OPPs to represent high standards of privacy protection. We suggest that business use of our guidelines when developing their OPPs would improve OPPs substantially. Our guidelines are preliminary, in that they are based upon the small sample of data explored, and are therefore unlikely to yield all of the issues or requirements for OPP guidelines. We believe, however, that we have provided a solid foundation upon which to build in future research.

We now turn to the situation in privacy practice, where surveys have highlighted the need to integrate OPP with actual privacy practice so that policies are indeed followed in practice (PAB, 2002c). Unfortunately, the only actual connection between OPPs and privacy practices found was the presence of privacy seals (for example, TRUSTe) on seven sites in 2002 – of which five had been present in
2000. Many privacy incidents have demonstrated, however, that the presence of a seal does not automatically imply adherence to policy (for example, the toysmart.com incident reported in Perine, 2000). Ideally, company policies should be translated into procedures and practices which are documented, thereby facilitating not only correct operationalisation of the policies, but also future audits and reviews. However it was not clear from the policies studied in either 2000 or 2002 that this translation to procedures and practice was occurring.

We believe there is a need for considerable guidance for companies in developing integrated online privacy policies, procedures and practices, and suggest that further research in this area would be highly valuable. With increasing exploitation of personal information through sophisticated data mining in CRM, and new privacy threats stemming from the need to address current and future global hostilities, we believe that making an effort to protect and assure personal privacy is of greater importance now than ever before, and urge businesses and researchers alike to continue a focus on what Warren and Brandeis labelled over a hundred years ago, in 1890, “the right to be let alone”.

REFERENCES


