Adding Value to Online Privacy for Consumers:
Remedying Deficiencies in Online Privacy Policies With an Holistic Approach

Authors:
Sharman Lichtenstein
Paula M C Swatman
Kanchan Babu

URL: http://www.deakin.edu.au/infosys/research/working_paper.htm
Adding Value to Online Privacy for Consumers:  
Remediing Deficiencies in Online Privacy Policies With an Holistic Approach

Sharman Lichtenstein¹, Paula M C Swatman² and Kanchan Babu³

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

²Faculty of Informatics, University of Koblenz-Landau, Germany  
paula.swatman@uni-koblenz.de

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

Abstract: Online privacy policies are important mechanisms for informing web site users about the level of information privacy protection afforded them when visiting web sites. To date, societal mechanisms and technologies have been the focus of attempts to improve the quality and effectiveness of online privacy policies. Little attention, however, has been given to the development and use of organisational measures for this purpose. In this paper 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 has identified broad areas of deficiency in existing online privacy policies, and offers a solution in the form of an holistic framework for the development, factors and content of online privacy policies for organisations. 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

Information privacy is the legitimate collection, use and disclosure of personal information, or “the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves” (Clarke, 1999). In our times, online privacy concerns continue to flourish within an atmosphere of general distrust of institutions and fears of technology abuse (Agre and Rotenberg, 1997). The main issues are intrusions, manipulation and discrimination; third party capture of personally identifiable information (PII); and identity theft and stalking (Westin, 2001). Online privacy, as a significant factor in consumer trust, is an imperative for e-business success (Harris Interactive, 2002; Hoffman et al, 1999). However, its provision is at odds with organisational goals such as the maximisation of personal information resource value obtained from disclosure to third parties (often for commercial gain), and retaining of customer loyalty via enhanced personalised service. Compounding this problem, user online privacy needs are frequently inconsistent with important societal values such as freedom of information, or public health and safety (Etzioni, 1999). In attempting to resolve these conflicting perspectives, considerable effort has been expended in seeking societal, national, organisational and technical solutions which can provide a balance of online privacy regarded as fair—from individual, societal, national and organisational perspectives.

The online privacy policy (OPP) (or privacy statement) is a key organisational measure for assuring online privacy for web site users (Chung and Paynter, 2002; Lichtenstein, 2001; OPA, 2002). These policies articulate the collection, use and protection of user personal information, as well as the choices offered to users in exercising their rights in respect of the control of their own personal information. The policies are intended to represent fair information privacy practices, as first defined by the OECD (1980), and later modified and extended by individual countries in order to accommodate perceived e-business and globalisation demands (for example, NPP, 2000; FTC, 2000).
To date, OPPs have a poor record in providing online protection. Studies conducted in the past few years showed that significant proportions of American and Australian OPPs failed to comply with recognized fair information practice principles—and overall, were ineffective (Anton and Earp, 2001; Babu, 2000; Culnan, 1999; enonymous, 2000; EPIC, 1999; Fox et al, 2000; FTC, 2000; Freehill Hollingdale & Page, 2000; Harris Interactive, 2002). These studies found that OPPs, terms of service, conditions of use, and other online policies with information privacy ramifications, were frequently overlooked by users in their eagerness to gain access to online products and services. Typically, users either signalled 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. Disturbingly, OPPs were found to be inconsistent with actual business privacy practices, as well as being poorly linked to business strategy and operations in general.

A recent report indicating some improvement in the quality of US OPPs (PFF, 2002) is interesting in light of the much-debated lack of privacy legislation in the US, where much has been expected from industry self-regulation, coupled with increased levels of public awareness, to bring about the changes desired. Australian OPPs have also improved in quality to some extent, according to an evaluation performed in February, 2001—a date well in advance of the recently enacted privacy legislation compliance deadline of December that year (Anderson, 2001). Nevertheless, in tandem with these positive indicators, well-publicized privacy violations continue to fuel public anxiety over privacy issues, with blame often ascribed in no small measure to ineffective OPPs (CNET, 2002; Maimelli, 2002).

In order to promote the effectiveness of OPPs and consumer confidence in them, a range of societal and technological measures are available. Privacy policy enforcement via co-regulation (for example, Australia) or self-regulation (for example, the US) are alternative approaches although, in the US, some type of legislation now appears inevitable (EPIC, 2002; FTC, 2000; Hollings, 2002). In a recent poll, consumers identified “third party verification that a company’s privacy practices match its OPP” as the single most important step a company could take toward securing consumer trust (Harris Interactive, 2002). Existing mechanisms for this purpose include privacy certification and seals such as TRUSTe and APCC (2001), as well as independent audits. P3P technology allows users to view a translated version of an OPP in a more usable form (W3C, 2002) and matches user privacy preferences with site privacy. However, critics of this approach point to the limitations of any technological translation of OPP and their matching with user online privacy needs—and observe that to date, few companies have adopted this approach (Harvey and Sanzaro, 2002).

Rather than relying upon societal and technological support for OPPs, organisations can provide more effective policies by employing appropriate guidelines in their development. Although various sets of guidelines already exist, we believe there are very good reasons for developing new, improved guidelines. Existing guidelines (for example, FTP, 2000; NPP, 2000; OPA, 2002) were not developed from empirical evidence, but were instead based on professional expertise, and may therefore have missed some of the issues, in this peculiarly dynamic and complex area. Some progress has been made toward developing empirically grounded, organisational guidelines. For example, Anton and Earl (2001) studied a set of health privacy policies using a goal search approach and identified a taxonomy of OPPs, although this did not account for contextual issues such as organisational and societal factors, and usability. Babu (2000) reported that existing sets of guidelines possessed some, but not all, of the desired characteristics. Finally, recent evidence suggests that existing OPPs are ineffective in managing the relevant risks (Sullivan, 2002), possibly due to deficiencies in current sets of guidelines.

In a companion paper, we presented the results of one part of a broad research project investigating online privacy policies—a complete, comprehensive set of organisational guidelines for OPPs, which businesses can utilize to develop their own OPPs (Lichtenstein et al., 2002). In this paper, we present the results and findings from a different part of the same research project. Here, our aim is to identify the commonly found deficiencies in existing OPPs, and recommend ways in which businesses can overcome them. Guidelines for OPPs can be useful not only for developing OPPs, but also for identifying their weaknesses—by acting as an instrument for measuring policy quality in specific areas, as well as for enabling the identification of trends and patterns which suggest the larger, often holistic problems—which in turn, demand holistic solutions. We employ our set of guidelines to these ends in this paper.

Following this brief survey of the literature and current research into online privacy protection, we summarise our research design. Next, we recap and summarise our guidelines for effective online privacy policy—based on the findings of Babu (2000), which we have extended via additional empirical investigations. We then discuss deficiencies in existing OPPs. As the culmination of our research study, we present an holistic framework for online privacy policies. Finally, we summarise and draw conclusions.
2. Research design

This longitudinal study was conducted in two stages, two years apart. In 2000, a literature review yielded a first-cut conceptual model of guidelines for OPP (Babu, 2000), for the purpose of exploring the topic further. A critical analysis of ten OPPs residing on the web sites of eight American businesses and two Australian businesses, was performed. These sites were chosen because they were dynamic, recognized e-business sites at the time of study, and because they featured substantial OPPs. The OPPs were evaluated for compliance with the first-cut guidelines in order to identify deficiencies for which solutions could be sought, and as a strategy for identifying unexpected, novel and useful elements within existing OPPs which could then be incorporated in future revisions of guidelines. Guideline compliance was measured by the presence of a reasonable implementation of it within a policy.

The policies were then analysed contextually, by studying the influence of HCI, organisational and human factors, and other issues, on the quality of the policies. A cross-policy analysis elicited trends, patterns and differences. To capture the relationship between an OPP and its organisational context, Babu conducted an in-depth case study of a recognized Australian online retailer—termed OzESale—via semi-structured interviews and document collection. As a result of these empirical investigations, Babu produced a revised, improved set of guidelines for OPP (Babu, 2000).

In the second stage of this project—our extension in 2002 of the original investigations—we reviewed recent literature, as well as the original research data and results, including the guidelines. We then analysed the nine still existing OPPs in their updated forms in April, 2002, for guideline compliance and contextual issues—again identifying trends, patterns and differences. We arrived at a set of guidelines for effective OPPs and identified major areas of deficiencies in current OPPs, leading us to a solution in the form of an holistic framework for online privacy policies for organisations.

3. Organisational guidelines for online privacy policy

In this section we summarise a comprehensive set of high level guidelines for online privacy policies, using 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 Babu, 2000; Anton and Earp, 2001; NPP, 2000; FTC, 2000; and our own empirical studies). Note that not all guidelines included in our categorization 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. The guidelines can also be utilized as a means for evaluating OPPs and identifying weaknesses which need addressing—a use for which we employ them in the next section.

By way of introduction, we provide a brief summary in this section of the overall results of a longitudinal comparison of OPPs in the two different years (full details of the comparison are found in Lichtenstein et al., 2002). In general, we found that the OPPs studied in 2000 had improved in quality over the period to 2002. We attribute this positive trend primarily to an increased consciousness of online privacy issues within the e-business community, combined with the effects of privacy legislation or industry self-regulation, based on recognized, fair information practices. Despite our finding of overall improvement in quality since 2000, we nevertheless found various deficiencies, in that many guidelines were inadequately addressed or missing, in the OPPs studied in 2002. In the following section, we discuss the main areas of deficiency arising from our investigations.

4. Deficiencies in online privacy policies

We have identified the following issues as the major deficiencies in current online privacy policies. We generalise in this discussion only in order to highlight the problems. We wish to point out that not all policies studied exhibited all the weaknesses described below—but, rather, that those deficiencies presented here are the main types found across the policies, overall.

- **User awareness**

Although companies have clearly made inroads into providing useful features and information in OPPs to assist users in becoming more aware of the privacy issues arising from site visits, there is still substantial room for improvement. The most fundamental type of awareness to provide is that of the importance and meaning of the OPP itself. Many people do not know what an online privacy policy (or privacy statement) is, nor realize its significance, and may overlook it for these reasons. Sites currently provide little awareness of the importance of this policy, nor do they direct users to it. “Terms of agreement” are often highlighted at the commencement of a
site visit, although the OPP is rarely drawn to the user’s attention. At the next level, most sites provide a basic awareness of the policy’s existence and how to locate it, via conspicuous links to the OPPs on each page, in a consistent position. However, on occasions when privacy threats are more likely to occur—either with or without the user’s awareness of the imminence of the threat (for example, on those occasions when personal information is being requested of the user)—few sites provide prominent links to their OPPs (for example, in a position adjacent to data collection boxes).

The quality of the language expression provided by OPPs needs far more attention. Currently, the English is too complex, and replete with “legalese”, ambiguity, inconsistencies, confusion and use of the words “most”, “many”, “some” etc—all of which can be used to hide exceptions which are not subject to the same rules. Many users do not understand the particular meaning of privacy terms used, for example, “disclosure”. The net effect is to hide the facts from the users, rather than making them aware of how their personal privacy is really being handled.

Current OPPs do not fully inform users about personal information collected. Policies do not provide complete lists of personal information that may be collected during site visits (nor, indeed, at later stages, via tracking through cookies, or code secretly stored on user computers)—hiding behind conditional clauses such as “Depending on what you purchase, we may also need to collect other personal information, like your clothing size...”. Policies do not fully inform users of the purpose of such collection, using general clauses such as “We use that information to service your account and to personalize your experience at...”. Finally, policies do not articulate the different third parties to whom personal information is disclosed, nor the purposes and uses of information so disclosed by those third parties, once they have the information in their possession. Confounding the user about disclosure practices is 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. Sites provided little in the way of informing users about the level of protection afforded at third party sites linked to by the site, as well as at other third parties with whom personal information could be shared at some future time. We address third party involvement as an important issue in its own right, later in this section.

Consumer education for the purpose of increasing user awareness of online privacy issues is currently very limited indeed, and we discuss this important issue separately also, later in this section.

- **Usability issues**

  OPPs pay scant attention to usability issues, which are always important in user interfaces, and particularly so in privacy interfaces (Babu, 2000; Greenberg, 1999; Lau et al, 1999). 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). However, OPPs are notoriously ambiguous, difficult to read, full of “legalese”, poorly structured, and generally difficult to understand. Overall, the policies are hindered by poorly designed HCIs—some more so than others.

- **Threats, risks and vulnerabilities**

  OPPs typically neglect to articulate online privacy threats, provide a risk assessment for these, or provide information about the vulnerabilities of the users’ personal information to privacy threats, although such information would clearly be of great interest to users. We did, however, find several exceptions to this rule. Notably, eBay features a vulnerabilities scenario analysis which provides useful information in this respect.

- **User roles and responsibilities**

  Very little information about user roles and responsibilities is provided in policies. Some improvements in this area have taken place in the two years since the earlier study, indicating that companies are now more aware of this important aspect of OPPs. In some policies, users are advised to safeguard their passwords, and to sign off and close browsers at the end of accessing the sites. In most cases, significant user roles and responsibilities (with respect to managing their online privacy) are not stated in the OPP but instead are found in other online policies, such as “terms of use”. Finally, we believe it would be very difficult for users to identify their responsibilities with respect to managing their online privacy in current OPPs, as the various specified user responsibilities are spread throughout the policies, in piecemeal fashion.
• **Control and choice**

Users are not in control of their personal information. Rather, the companies exercise almost all control, a situation which is unlikely to engender user confidence. In particular, users lack sufficient, consistent consent opportunities, with respect to the provision, disclosure or use of their personal information. Most policies offer complex combinations of opt-out and opt-in within their OPPs, which can be confusing. Furthermore, consent is 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”.

• **Data quality**

Although users are usually offered some type of access to OPPs for the purpose of checking and correcting their personal information, in many cases the user is only provided with a contact email address, rather than an online form to update immediately. Furthermore, all responsibility for data quality assurance “appears” to be with the user, with none overtly guaranteed by the company (in the OPP), other than assurances relating to security threats.

• **Links to privacy practices**

The only overt linkage between the OPP and actual business privacy practices is the presence on the site of a privacy seal, which many companies do not possess. In our case study of OzeSale in 2000, there appeared to be very little connection between policy and practices—a clear cause for concern. Normally, company policies are translated into procedures which are documented and then followed, thereby facilitating not only correct implementation of the policies, but also future audits and reviews. It was not clear from the policies that this translation to procedures was occurring and indeed, at OzESale, it was not. We also observed, through our study of OzESale, some indication as to why organisations may not be following their online privacy policies in practice (many such policy violations have been widely reported). It appears that privacy infrastructures within companies are not yet powerful enough, or sufficiently developed to enforce their privacy policies inside the companies themselves, although this may be changing with the recent trend toward establishing organisational Privacy Officer functions and privacy certification via annual audits.

• **Consumer education**

There is a lack of understanding of the issues provided by policies, for consumers. For example, consumers cannot find answers from existing OPPs to the following questions: “What are online privacy policies?” “What will happen if I ignore them?” “Are privacy statements and terms of use the same things?” “What does personally identifiable information mean?” “What is a third party disclosure?” “Can someone find me from my personally identifiable information?” —and so much more.

• **Flow of personal information**

Cookies used for monitoring/tracking purposes are given only cursory explanations in policies—not extensively or clearly enough for the average user. Sites often make some commitment to explain their use of cookies as a form of monitoring or tracking for the purpose of better serving the user, although the user isn’t given a genuine choice much of the time to refuse cookies—because, without them, many site features simply will not be provided. We feel this is an unethical business practice, as the user will be all too often easily swayed into accepting the cookies in order to obtain the desired services.

Information about personal information aggregation, storage, transfer, disposal and personalisation is scanty, missing or exhibits other problems, as follows. There are inconsistencies—for example, one policy stated in one section that anonymous (ie non PII, such as IP address) information would not be linked to the user’s PII without their consent (ie 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 (ie there was no user choice). There are omissions—for example, regarding information storage, only data quality or security issues were addressed in policies, and the duration of storage was not made explicit in most cases, in either year. There was cause for concern, for example, “Information collected at this site may be disclosed to third parties where functions are being outsourced”. There were generalities and vagueness, for example, “information collected is used to provide the customer with better service”.

---

S Lichtenstein, P M C Swatman, K Babu
<table>
<thead>
<tr>
<th>Guideline Category</th>
<th>Brief Description of Guideline</th>
<th>Guideline Within Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Awareness</td>
<td>The site should facilitate user awareness of its privacy policies.</td>
<td>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</td>
</tr>
<tr>
<td>2. Data quality</td>
<td>Personal information should be maintained as complete, timely and correct, by the company.</td>
<td></td>
</tr>
<tr>
<td>3. Security</td>
<td>Personal information should be secured wherever possible.</td>
<td>3.1 Data security 3.2 Data transmission 3.3 Cookies</td>
</tr>
<tr>
<td>4. Information movement</td>
<td>Details of personal privacy provided in various states of information movement should be provided to the user.</td>
<td>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</td>
</tr>
<tr>
<td>5. User identification</td>
<td>Use and disclosure of a user’s site identifier as either PII, anonymous, pseudonymous, should be stated.</td>
<td>5.1 User identifier 5.2 Anonymity 5.3 Pseudonymity 5.4 Nonrepudiation</td>
</tr>
<tr>
<td>6. Accountability</td>
<td>Company and user should be held accountable for actions.</td>
<td>6.1 Enforcement 6.2 User responsibilities</td>
</tr>
<tr>
<td>7. User access</td>
<td>Users should have opportunity to participate in their personal information protection as necessary.</td>
<td>7.1 User access and self-correction 7.2 User access to other user data</td>
</tr>
<tr>
<td>8. Assurance</td>
<td>Policies should state ways in which companies assure users they are following their OPPs in practice.</td>
<td>8.1 User recourse 8.2 Verification 8.3 Consequences</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.</td>
<td></td>
</tr>
<tr>
<td>10. Choice</td>
<td>The user should be given choices with respect to collection and use of personal information.</td>
<td>10.1 Consent</td>
</tr>
<tr>
<td>11. Change management</td>
<td>Companies require procedures for change management of their OPPs.</td>
<td>11.1 Evolution 11.2 Changes to policy 11.3 Change of company control</td>
</tr>
<tr>
<td>12. Children’s Privacy</td>
<td>The policy should provide information regarding access by, and involvement of, children.</td>
<td></td>
</tr>
<tr>
<td>13. Sensitive information</td>
<td>The ways in which sensitive information (eg religion) is treated differently to other personal information, should be explained.</td>
<td></td>
</tr>
<tr>
<td>14. Exceptions</td>
<td>Exceptions to the OPP policy should be clearly stated.</td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Summary of guidelines for online privacy policy (Lichtenstein et al., 2002) (compiled from Babu, 2000; Anton and Earp, 2001; NPP, 2000; FTC, 2000 and our empirical studies)
Transborder personal information flow is often not addressed by policies at all, so that users would not be aware of what level of protection would be provided should their personal information move across a state or national border into another legal jurisdiction.

- **Change management**

  Users are unable to consult their OPP history with respect to a particular site. We did not find even one OPP which provided this facility in our study—a deficiency 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.

- **Relationship to other company policies**

  There is a great deal of confusion for a user who is attempting to ascertain the relationship between the OPP and other online and offline company policies. There are no answers in OPPs or in other areas of sites, to 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?” At present, businesses appear to be dumping their OPP 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. We also 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.

- **Data transmission vulnerabilities**

  Users are not made aware of the specific nature of threats to their data during transmission, such as interception, eavesdropping and masquerading. Most policies issued a disclaimer to the effect that security across the Internet is never, and could never be, 100% secure.

- **Third party privacy protection**

  Although most sites summarise privacy protection information about third party sites linked to, as well as about third parties to whom information could be disclosed by the company through private negotiations (ie third parties not hyperlinked to the site)—the information provided is often just a disclaimer, rather than any kind of assurance.

- **User identification**

  User identification issues about the use and disclosure of a user’s site identifier as either PII, anonymous, or pseudonymous, are rarely addressed—and where they are addressed, are poorly explained. 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 such as TRUSTe.

- **User recourse**

  Policies provide little information about the types of grievances consumers may have, and when it would be appropriate to contact the company regarding these. The methods of contact provided are not always convenient for the user. For example, a policy listing a US phone number when the user is located in Australia, is clearly inconvenient and inappropriate from the user perspective.

5. **An holistic approach to online privacy policy**

  We observed throughout our study, as well as in our analysis of deficiencies in the previous section, the interplay of many different types of factors in the topic area of OPP. In recent years, there has been a growing recognition of the need for holistic security and system solutions which integrate the human, social, organisational and technical issues (Baskerville et al, 2000; Lichtenstein, 2001; Lichtenstein and Swatman, 2001). On reviewing the many diverse issues raised in the guidelines as well as in the analysis of deficiencies in the previous section, we propose an holistic framework for online privacy policy (Figure 1) comprising three sets of guidelines—a set of factors to be considered when developing the policy, a method for the development of the policy, and a set of guidelines for the content of the policy (Table 1). Our framework is an adaptation of the framework for Internet security policy developed by Lichtenstein (2001).
The original framework for Internet security policy included the online privacy policy as a sub-policy of the Internet security policy, suggesting that the framework may well be adaptable for use with online privacy policies. Currently, we have not developed models for the components shown in Figure 1—except for the Content model, which is represented by our set of guidelines (Table 1).

![Diagram of Online Privacy Policy Framework]

Figure 1. Framework for Online Privacy Policy

Clearly, a model which articulates the online privacy risks to be considered when developing the policy, would be useful—while models for the different types of factors in the factors model (organisational, administrative, legal, societal, technical, standards and human issues) would also play a helpful role in enabling businesses to identify all the important issues that need to be taken into account in OPP development. Figure 1 shows the development of the OPP by performing a risk assessment of the identified online privacy risks as they impact the business privacy data, in order to identify the high risk online privacy threats to be addressed in the policy. Other factors are also taken into account, as are the content model (our guidelines in Table 1) and existing company policies (“org policies” and “Internet security policy (ISP)” in the diagram) in order to develop the OPP.

6. Summary and conclusions

In this paper, we have reviewed the issues in online protection via online privacy policies, and summarised a set of high level organisational guidelines for companies to utilize in the development of an OPP. We provided a descriptive analysis of the deficiencies observed in Australian and US OPPs in 2000 and 2002, which companies can use to improve their future policies. As the culmination of this stage of our research project, we proposed an holistic framework for online privacy policy—which incorporates our guidelines, and includes a risk-based method for developing the policy, as well as a model of the types of factors to be considered in policy development. We suggest that this framework would prove useful to businesses in its current form, but far more so when developed to a greater depth. Currently, it is a very preliminary piece of research, requiring further exploration and refinement.
Although our results were 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 indicate there has been a significant improvement in the quality of OPPs over the period 2000-2002, which we attribute to increased public awareness of the issues, combined with co-regulation (Australia) or industry self-regulation (US). Nevertheless, there is still a significant shortfall between policies, and the requirements for such policies as indicated by our guidelines. Businesses need to set as a priority the improvement of their online privacy policies for a multitude of reasons—including raising ethical business standards online, “doing the right thing” by their online customers, and securing the elusive consumer trust component that can provide business success. Privacy is an area of considerable concern to many online consumers (Harris Interactive, 2002), and those companies which provide adequate support for their customers’ privacy – and particularly those which present this information in an effective manner – increase the likelihood of consumer loyalty. As safety is the crucial issue today for airlines, so may privacy become for online businesses in the next decade.

7. References


