Adding Value to Online Privacy for Consumers: Remedying Deficiences in Online Privacy Policies with an Holistic Approach

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

Paula M C Swatman
Faculty of Informatics, University of Koblenz-Landau, Germany, and
School of Information Systems, Deakin University, Australia
paula.swatman@uni-koblenz.de

Kanchan Babu
Telstra Retail, Melbourne, Australia
Anitha.babu@team.telstra.com

Abstract

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 organizations. 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 claims of individuals that data about themselves should generally not be available to other individuals and organizations, 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" [1]. In our times, consumer online privacy concerns continue to flourish within an atmosphere of general distrust of institutions and fears of technology abuse [2, 3]. A recent survey identified the main concerns as intrusion, manipulation and discrimination; third party capture of personally identifiable information (PII); and identity theft and stalking [4].

Online privacy, a significant factor in consumer trust, is increasingly being viewed as an imperative for e-business success [3, 5]. However, its provision is often at odds with organizational goals—such as the maximization of personal information resource value obtained from disclosure to third parties (often for commercial gain) and the retention of customer loyalty via enhanced personalized services. Confounding this issue, user online privacy needs are frequently inconsistent with other important societal values, such as the free flow of information, public health and safety [6]. In attempting to resolve these conflicting perspectives, considerable effort has been expended seeking societal, organizational and technical solutions which can provide a balance of online privacy regarded as fair—from individual, societal and organizational perspectives.

The online privacy policy (OPP) (or privacy statement) is a key organizational measure for assuring online privacy for web site users [7, 8, 9]. 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

Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03)
0-7695-1874-5/03 $17.00 © 2002 IEEE

defined by the OECD [10], and later modified and extended by individual countries in order to accommodate perceived e-business and globalization demands [for example, 11, 12].

To date, OPPs have a poor record in providing online protection. Studies conducted in the past few years revealed that significant proportions of US and Australian OPPs failed to comply with recognized fair information practice principles and overall, were ineffective [3, 12, 13, 14, 15, 16, 17, 18]. 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 privacy practices, and poorly linked to business strategy and operations in general.

A recent report indicating some improvement in the quality of US OPPs is interesting, in light of the controversial lack of privacy legislation in the US, where much has been expected from industry self-regulation combined with increased levels of public awareness, to effect desired changes [19]. Australian OPPs have also improved, according to one investigation in February, 2001—a date well in advance of the recently enacted privacy legislation's compliance deadline of December that year [20]. 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 [21, 22].

In order to promote the effectiveness of OPPs and consumer confidence in them, a range of societal measures is available. Privacy 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 [12, 23, 24]. A new focus was suggested by a recent poll, in which consumers identified "third party verification that a company's privacy practices match its OPP" as the single greatest step a company could take toward securing consumer trust [3]. Existing verification mechanisms include privacy certification and seals such as TRUSTe and APCC [25], as well as independent audits.

Technological support for OPPs is now available. A landmark development has been P3P, which enables consumers to view a translated version of a site's OPP in a more usable form, and enables comparisons of consumer privacy preferences with the policy's privacy levels [26]. However, critics have debated the limitations of this approach, and observe that to date, few companies have adopted this technology [27].

To complement societal and technological support for OPPs, organizational guidelines can be used. Although various sets of guidelines already exist, we believe there are very good reasons for developing new, improved guidelines. Existing guidelines [for example, 9, 11, 12] 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. Babu [14] reported that existing sets of guidelines possessed some, but not all, of the desired characteristics. Furthermore, recent evidence suggests that existing OPPs are ineffective in managing related risks, possibly due to deficiencies in current sets of guidelines [28].

Some progress has been made in developing empirically grounded, organizational guidelines. For example, Anton and Earp [13] studied health privacy policies using a goal search approach, resulting in a taxonomy of OPPs—although this, however, did not account for contextual issues such as organizational and societal factors, and usability.

In a companion paper, we presented the results of one part of a broad research project investigating online privacy policies—a high level set of organizational guidelines for OPPs [29]. In this paper, we present results and findings from a different part of the same research project. Here, our aim is to identify commonly found deficiencies in existing OPPs, and recommend organizational solutions. 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, and highlighting trends and patterns suggesting 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 and the role of OPPs, we overview our research design. Next, we recap and summarize our guidelines for effective online privacy policy. Deficiencies in existing OPPs are then identified and analyzed. As the culmination of our study, we provide an holistic framework for online privacy policies. Finally, we review our work, 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, for the purpose of exploring the topic further [14]. A critical

analysis of ten OPPs residing on the web sites of eight American businesses and two Australian businesses, was performed. The sites were chosen because they were dynamic, recognized e-business sites at the time of study, and because they featured substantial OPPs. 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 services, one travel and three entertainment companies.

First, the OPPs were evaluated for compliance with the first-cut guidelines in order to identify deficiencies, and as a strategy for discovering unexpected, novel and useful elements within existing OPPs which could later be incorporated in future revisions of guidelines. Guideline compliance was measured by its reasonable implementation within a policy.

The policies were then analyzed contextually, by studying the influence of human computer interaction, organizational and human factors, as well as 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 organizational context, Babu [14] 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 [14].

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, reanalyzed the original research data, and reviewed the original guidelines and results. We then analyzed 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. We thus arrived at a final set of guidelines for effective OPPs (Section 3), and identified major areas of deficiencies in current OPPs (Section 4), leading us to a solution in the form of an holistic framework for online privacy policies for organizations (Section 5).

3. Organizational guidelines for online privacy policy

In Table 1, we summarize 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 [11, 12, 13, 14] and our own empirical studies).

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. Note that not all guidelines included in our categorization are addressed by various sets of existing fair information practices and regulations, although our study suggests that all our guidelines are important, and therefore worthy of inclusion in our final set.

By way of introduction, we briefly comment on the overall results of the longitudinal comparison of OPPs in the two different years (full details are in a forthcoming journal article, currently under review). We found the OPPs for 2002 had generally improved in quality since 2000. 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, we nonetheless identified various deficiencies, in that many guidelines were inadequately addressed or missing in the OPPs studied in 2002 (as were many in 2000). In the following section we discuss the main areas of deficiency in OPPs, arising from our investigations. We also highlight changes in the policies over the two year period.

4. Deficiencies in online privacy policies

We generalize in the following discussion only in order to highlight the problems. We point out that not every policy studied exhibited all of the weaknesses described below—but rather, that those deficiencies presented were the *main* types found across the policies, overall.

4.1 User awareness

Although companies have clearly made inroads since 2000 into providing useful features and information in OPPs in order 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, all sites (in both 2000 and 2002) provided a basic awareness of the policy's existence and

Table 1. Summary of guidelines for online privacy policy (compiled from [11, 12, 13, 14] and our own additional studies)

Online Privacy Policy Guideline Category	Brief Description of Guideline Category	Guideline Within Category
1. Awareness	The site should facilitate user awareness of its privacy policies.	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 personalization 4.7 Transborder data flow
5. User identification	Use and disclosure of a user's site identifier as either PII, anonymous, 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	Policies should state ways in which companies assure users they are following their OPPs in practice.	8.1 User recourse 8.2 Verification 8.3 Consequences
9. Contact	Policies should state how, and for what purpose, organizations contact users using PII to make the contact.	
10. Choice	The user should be given choices with respect to collection and use of personal information.	10.1 Consent
11. Change management	Companies require procedures for change management of OPPs.	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 (eg religion) is treated differently to other personal information, should be explained.	
14. Exceptions	Exceptions to the OPP policy should be clearly stated.	

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)—only a few sites provided prominent links to their OPPs (for example, in a position adjacent to data collection boxes). This still represents an improvement since 2000, when none of the sites provided this facility.

The quality of the language expression provided by OPPs needs far more attention. Currently in seven out of nine sites, the English is too complex, and replete with "legalese", ambiguity, inconsistencies, confusion and use of the words "most", "many", 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.

OPPs do not *fully* inform users about personal information collected, although small improvements since 2000 were observed in this regard. Eight out of nine policies in 2002 did not provide complete lists of personal information that might 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..". None of the policies fully informed users of the purposes of such data collection, instead using general clauses such as, "We use that information to service your account and to personalize your experience at ...". Finally, eight out of nine policies did 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 was common to most policies. 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 screen. Most policies did not provide enough information 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.

4.2 Usability issues

OPPs pay scant attention to usability issues, which are always important to the effectiveness of user interfaces, and particularly so in privacy interfaces [14, 30, 31]. Usability has been identified as an important factor in all types of online policies for the securing of consumer trust [32, 33]. As mentioned in Section 4.1, we found all the OPPs in 2002 to be confusing, ambiguous and difficult to follow, in places. Most policies used "legalese", and most were poorly structured with respect to indexing or navigation. Overall, the policies exhibited poorly designed human computer interfaces—some more so than others. There was still noticeable improvement since 2000, however, when the language and layout were significantly worse in almost all the policies.

4.3 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. Almost all the policies analyzed did not provide these features either in 2000 or 2002, suggesting that much improvement is still needed in this area. We did, however, discover several exceptions in our study. Most notably, eBay featured a vulnerabilities scenario analysis which provides useful information in this respect.

4.4 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, however there is still room for much improvement. 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.

4.5 Control and choice

According to all the OPPs studied in both 2000 and 2002, users are not in control of their personal information. At present, all the companies studied exercise almost all the control, a situation which is unlikely to engender user confidence. In particular, all the studied sites' users lack sufficient, consistent choice (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, which can be confusing. Furthermore, choice/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". Encouragingly, the amount of choice provided in 2002 had increased significantly in almost all policies, since 2000.

4.6 Data quality

Although in all policies in both years, users were offered some type of access to OPPs for the purpose of checking and correcting their personal information, in most cases the user was only provided with contact details, rather than an online form to update immediately. Furthermore, all responsibility for data quality assurance appeared to be with the user, with none guaranteed by the company, other than assurances relating to the security of collected personal information.

Regarding security, five OPPs in 2000—increasing to all nine in 2002—provided some type of 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, "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".

By 2002, two of the OPPs listed extensive security provisions, while other sites had added to theirs. For example, one OPP assured: the use of secure connections from customer browser to company site, encryption for sensitive personal information, logical security of databases on company systems, access restrictions to such databases, employee corporate data confidentiality contracts, and quality assurance procedures to ensure product development did not compromise existing privacy protection. We view this as a promising trend.

4.7 Links to privacy practices

The only overt linkages between the OPP and actual business privacy practices were the presence in 2002, on seven of the sites, of privacy seals (for example, TRUSTe)—of which only five had been present in 2000. In our case study of OzeSale in 2000, there appeared to be very little connection between policy and actual 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 organizations 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 organizational Privacy Officer functions and privacy certification via annual audits.

4.8 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 third party disclosure?", "Can someone find me from my personally identifiable information?"—and much more.

In 2000, only one policy provided links to educational and consumer privacy sites for consumer education, while this number rose to four policies in 2002. However, we believe that much more than mere links to external informational sites is needed.

4.9 Flow of personal information

Cookies used for monitoring or tracking purposes were given only cursory, unsatisfying explanations in all policies. This situation remained unchanged between

2000 and 2002. Sites often make 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 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 personalization is scanty, missing or exhibits other problems, appearing in few policies in both 2000 and 2002, as follows. There are inconsistencies—for example, one policy stated in one section that anonymous (i.e. non PII, such as IP address) information would not be linked to the user's PII without their consent (i.e. 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 (i.e. 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".

Transborder personal information flow was only addressed by a few policies in both years, and even then, the advices were merely disclaimers. Users of all policies studied would not be aware of the level of personal information protection afforded should their information move across a state or national border into another legal jurisdiction, unless they carried out their own investigations.

4.10 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 [22]. Yet some of these users were convinced they had never given such permissions.

An increasing trend we observed is for companies to update their policies frequently, making it even more difficult for consumers to keep abreast of changes.

4.11 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 were no answers in any of the OPPs studied, or in other areas of sites, to questions such as: "What is the relationship between an organization'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 OPPs 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 suit 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.

4.12 Data transmission vulnerabilities

Users were not informed in either year about specific data transmission threats such as interception, eavesdropping and masquerading, in any of the policies. However by 2002, most of the policies issued a disclaimer to the effect that security transmitted across the Internet is never, and could never be, 100% secure, and therefore information in transmission will always be vulnerable.

4.13 Third party privacy protection

Although most of the sites summarized 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 (i.e. third parties not hyperlinked to the site)—the information provided was often just a disclaimer, rather than any kind of assurance. Interestingly, the number of policy disclaimers in 2002 regarding privacy levels at linked third party sites had doubled since 2000, from four to eight policies, however more than mere disclaimers is

needed. Disclaimers in 2002 tended towards "encouraging" users to consult third party policies.

4.14 User identification

User identification issues about the use and disclosure of a user's site identifier as either PII, anonymous, or pseudonymous, were not addressed by most policies in either year—and in the few policies where they were addressed, were poorly explained.

4.15 User recourse

Most 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. The OPPs in our study did not address how the companies would incur sanctions if they failed to comply with their policies.

Other recourse was provided by the presence of privacy seals such as TRUSTe (refer Section 4.7). Where a seal is on a site—for example, the Australian Privacy Seal—the consumer can complain to a representative about a perceived policy infringement, and the seal can be revoked if the company has indeed breached policy.

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, organizational and technical issues [8, 34, 35]. 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 e-business security policy developed by Lichtenstein [8]. The original framework for e-business security policy included the online privacy policy as a sub-policy of the e-business 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). Clearly, an online privacy risks model which articulates the range of potential online privacy risks to be considered when developing the policy, would be useful—while individual models for the different types of factors depicted in the Factors model (organizational, 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.

The unique position of the Human Issues in the Factors model is deserving of special comment. In the work of Lichtenstein [8] it was found that the various non-human issues in all types of e-business security policies needed to be viewed through the lens of the important human issues involved. This research study suggests that the same is true for online privacy policies—with technologies, administrative, organizational and other issues, all needing to be tempered by the diverse needs of the all important individuals for whom the privacy is being provided, before appropriate sub-policies can be developed.

Figure 1 includes a model for the development of the OPP in the top left hand corner, and includes a risk assessment of online privacy risks as they impact the specific business privacy data, in order to identify the significant online privacy risks to be addressed by the policy. Other factors (from the Factors model) are also taken into account, as are the structure provided by the OPP content model (our guidelines in Table 1) and the integration of existing company policies ("org policies" and "e-business security policy (ESP)" 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 focusing on online privacy policies, and summarized a set of high level organizational 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 policies in the future.

As the culmination of this stage of our research project, we proposed an holistic framework for online privacy policy—which incorporates our guidelines as the basis of a structure for the OPP, 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 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 generalize from this small sample of data—our results indicate there has been a small but 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 that can yield e-business success. Privacy is an area of considerable concern to many online consumers [3], 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.

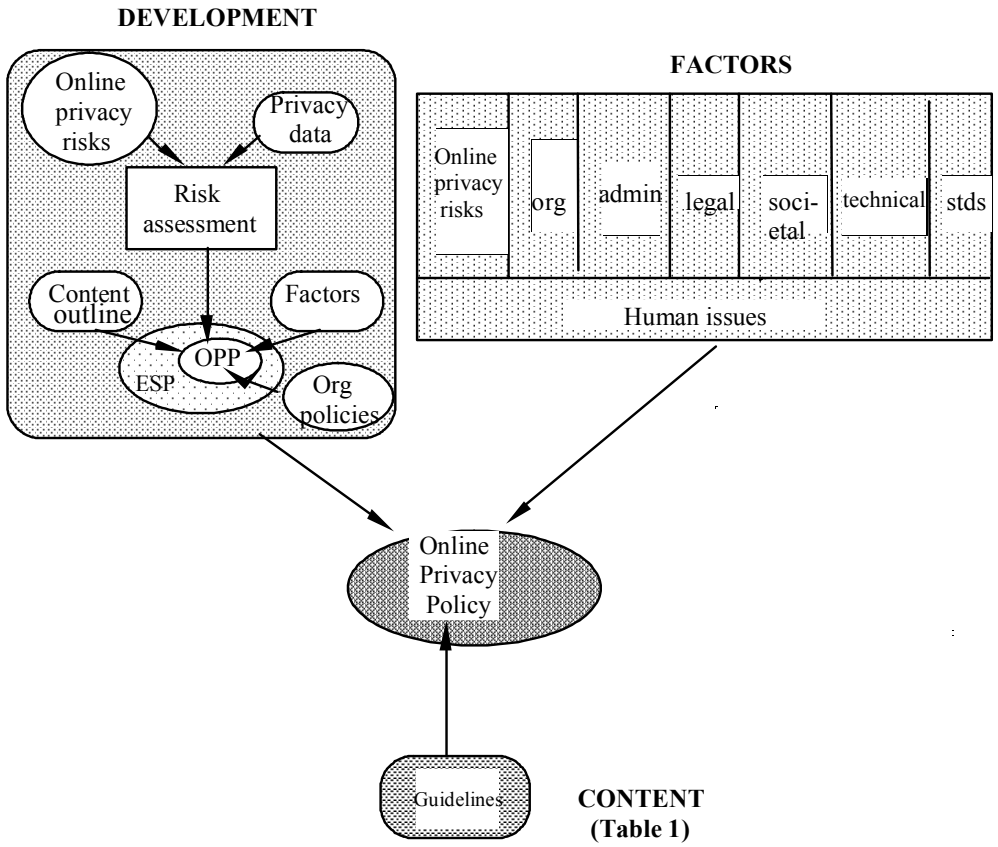

Figure 1. Framework for Online Privacy Policy

7. Acknowledgements

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

8. References

[1] Clarke, R. (1999) "Internet privacy concerns confirm the case for intervention", *Communications of the ACM*, 42 (2), February, pp 60-67.

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

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

[4] 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.

[5] Hoffman, D.L., Novak, T.P. and Peralta, M. (1999) "Building Consumer Trust Online", *Communications of the ACM*, 42 (4), April.

[6] Etzioni, A. (1999) *The Limits of Privacy*, New York: Basic Books.

[7] 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.

[8] Lichtenstein, S. (2001) *Internet security policy for organizations*, Thesis (PhD) (public version), School of Information Management and Systems, Monash University, Melbourne, Australia.

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

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

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

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

[13] Anton, A.I. and Earp, J.P. (2001) *A Taxonomy for Web Site Privacy Requirements*, 18 December, NCSU Dept. of Comp Science Technical Report, TR-2001-14.

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

[15] Culnan, M.J. (1999) *Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission*, The McDonough School of Business, Georgetown University, Washington DC, US.

[16] EPIC (1999) "Report Slams Privacy Policies; Poll Finds Privacy is Top Concern", *Epic Alert*, 5 (15).

[17] Fox, S., Rainie, L., Horrigan, J., Lenhart, A., Spooner, T. and Carter, C. (2000) *Trust and privacy online: Why Americans want to rewrite the rules,* The Pew Internet and American Life Project, Pew Research Center for People and Press, Washington, DC.

[18] Freehills (2000) *Internet Privacy Survey*, Freehills law firm, Melbourne, Australia.

[19] 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.

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

[21] Good, N.S. and Krekelberg, A. (2002) *Usability and privacy: a study of Kazaa P2P file-sharing*, Hewlett-Packard Labs, Technical Report, HPL-2002-163.

[22] Mainelli, T. (2002) "Hotmail Policy Raises Privacy Concerns", *PCWorld.com*, IDG.net, May 27.

[23] EPIC (2002) "Senate Considers Internet Privacy Legislation", *Epic Alert,* 9 (8).

[24] Hollings, E. (2002) *Online Personal Privacy Act*, US Government, US.

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

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

[27] Harvey, J.A. and Sanzaro, K.M. (2002) *P3P and IE 6: Raising More Privacy Issues Than They Resolve?* Gigalaw.com, February.

[28] Sullivan, B. (2002) *Ebay Privacy Policy Draws Fire—Again*, Computerworld, March 20.

[29] Lichtenstein, S., Swatman, P.M.C. and Babu, K. (2002) "Effective Online Privacy Policies", in *Proceedings of ACIS 2002, Thirteenth Australasian Conference on Information Systems*, Victoria University, Melbourne, Australia.

[30] Greenberg, I. (1999) "Facing Up to New Interfaces", *Computer*, IEEE, April, 32 (4), pp 14-16.

[31] Lau, T., Etzioni, O. And Weld, D.S. (1999) "Privacy Interfaces for Information Management", *Communications of the ACM*, 42 (10), pp. 88-94.

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

[33] Nielsen Norman Group (2001*) E-commerce User Experience: Design Guidelines for Trust and Credibility*, Nielsen Norman Group.

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

[35] Lichtenstein, S. and Swatman, P.M.C. (2001) "Effective Management and Policy in E-Business Security", in *Proceedings of Fourteenth International Bled Electronic Commerce Conference,* O'Keefe, B., Loebbecke, C., Gricar, J., Pucihar, A. and Lenart, G. (Eds), Bled, Slovenia.

.