2006

A Pilot Study of the Effectiveness of Privacy Policy Statements

Roger Clarke
Xamax Consultancy Pty Ltd, Australia, roger.clarke@xamax.com.au

19th Bled eConference

eValues

Bled, Slovenia, June 5 - 7, 2006

A Pilot Study of the Effectiveness of Privacy Policy Statements

Roger Clarke

Xamax Consultancy Pty Ltd, Australia
Visiting Professor at U.N.S.W., A.N.U. and University of Hong Kong
Roger.Clarke@xamax.com.au

Abstract

An expectation exists, particularly in the U.S.A., that B2C web-site operators will provide public notice of their practices in relation to the personal data that they hold. Such documents are referred to in this paper as 'privacy policy statements' (PPS). Privacy is an important element in consumer trust, and hence in a consumer's decision to make purchases using Internet commerce services. PPS could therefore be expected to play an important role in overcoming the impediments to consumer purchases online.

This paper adds to the growing research literature on PPS by developing a research design involving comparison of an organisation's PPS against a normative template. A pilot study of six B2C sites was undertaken, in order to assess the practicability of the design, and provide some initial substantive insight into the contributions that PPS currently make to consumer trust.

1 Introduction

The term Privacy Policy Statement (PPS) is used in this paper to refer to information provided by the operator of a B2C eCommerce web-site, to explain its practices in relation to the personal data that it gathers about consumers. Other equivalent terms include 'privacy policies', 'privacy statements', 'privacy notices', and 'information practice statements'.

PPS emerged in the U.S.A. in the mid-to-late 1990s. The U.S. has no generic private sector privacy legislation, with its Congress clinging to the belief that business should remain as unfettered as possible. The idea of self-regulation has been put forward as an alternative to genuine regulation of business activities. PPS were intended to be an element in that framework.

The use of PPS has spread, however, and they have come to be used in jurisdictions where data protection laws exist. When PPS are used within a formalised regualtory context, their purposes and impacts are rather different.

PPS have been studied from a number of perspectives. The research on which this paper is based adopts an approach different from prior studies. A pilot study was undertaken to evaluate a number of PPS against a normative template, in order to assess the extent to which they were likely to represent effective protection for consumers' privacy.

This is a further project in a long-running research program undertaken by the author in the area of privacy and information technology generally, in the context of the Internet in particular, and in B2C eCommerce specifically. 15 of the c. 70 citations are accordingly to prior refereed papers by the author. These provide fuller analyses and arguments supporting various points made in this paper, and many further references to the relevant literature.

The paper commences by reviewing the role of privacy as a trust factor in Internet-based B2C eCommerce. This is followed by a consideration of the various means whereby privacy can be protected. The role and nature of privacy policy statements is delineated, existing conventions are identified, and an evaluation template proposed.

A research design is developed to investigate the effectiveness of privacy policy statements from the perspective of consumers. This includes attention to the population of B2C services, population segmentation, and sampling frames. A small sample is selected, and a pilot survey conducted. The results provide a basis for refinement of the research design, and lay the foundation for conduct of a more substantial survey.

2 Privacy as a Trust Factor

According to the Theory of Reasoned Action (TRA) of Ajzen & Fishbein (1980), trust and risk are major determinants of attitude towards purchasing, and hence of intention to purchase. In the context of Internet-based B2C eCommerce, trust is usefully defined as confident reliance by one party about the behaviour of other parties.

The concept of trust originates in familial and social settings, where parties have considerable mutual understanding, mutual interests, and mutual dependence. These are difficult to replicate in merely economic relationships. In B2C eCommerce, trust is little more than what the consumer is forced to depend on when no other form of risk amelioration strategy is available (Clarke 2002a).

The strongest sources of trust arise from a pre-existing direct relationship between the parties, primarily kinship and mateship, but also to some extent in such commercial forms as principal-agent relationships, contract and multiple prior transactions. A less strong source is direct experience, as arises from a prior transaction, or perhaps prior exposure to the organisation concerned, e.g. by watching a trusted friend conduct a transaction. Weaker again is referred trust, such as 'word-of-mouth' and reputation. Still weaker are mere symbols of trust, which are often nothing more than contrived images, in the form of brands. The weakest form of all is 'meta-brands', such as accreditation and 'seals of approval', especially from industry associations that lack the power to regulate even their members let alone non-members (Clarke 2001b).

Trust is not easy to achieve in Internet contexts. The parties have little knowledge about one another, and cannot depend on such confidence-engendering measures as physical proximity, handshakes, body language, a common legal jurisdiction, or even necessarily any definable jurisdiction (e.g. Lee & Turban 2001, Clarke 2001c).

When business interests finally discovered the Internet in the mid-1990s, it was assumed that electronic commerce would explode. In fact, adoption was far slower than most

Internet growth metrics, because business failed to address the trust gap. This was examined in Clarke (1999b).

Trust issues are many and varied. Some are related to the terms of trade, especially their non-negotiability, their imbalance in favour of the vendor, the location of the contract in a jurisdiction that suits the vendor rather than the customer, and the lack of consumer protections that the consumer normally enjoys when purchasing goods and services in their home jurisdiction. Further concerns arise in relation to default by the vendor or by an intermediary such as a carrier. Yet more are security issues, relating to the consumer's identity and personal data, including the person's location and contact-points.

This paper is concerned with the particular cluster of impediments to the adoption of B2C eCommerce that are associated with privacy. Privacy is the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations. There are many dimensions of privacy. The one most relevant to the present context is personal data privacy. Key requirements include the individual's ability to prevent data about themselves being available to other individuals and organisations, and, where data is available, the ability to control its quality, use and further disclosure.

The role that privacy plays in the achievement of trust has been examined by various researchers (e.g. Palmer et al. 2000, Clarke 2001c, Belanger et al. 2002, Xu et al. 2003). The fundamental requirements are that the amount of personal data available to the marketer must be minimised, and such data as is available must be, and be perceived by consumers to be, protected against abuse by the marketer and others. This may be achieved through substantive measures combined with effective communication of their existence to consumers; or by effective communication based on as limited an actual set of constraints as the organisation can get away with. There are significance cultural differences in the importance placed on privacy, and its role in trust (e.g. Dinev et al. 2005, Kim 2005).

3 Privacy Protection Mechanisms

Several different approaches are taken to privacy protection. This section briefly reviews ways in which online marketers can design their business processes to be privacy-sensitive, and can use technology as an antidote as well as a threat. It culminates in a summary of the ways in which the law can be used to protect privacy.

3.1 Business Process Protections

Until the early-to-mid twentieth century, most consumer transactions were conducted in physical marketplaces. Judgements were made based on the information available at the time the decision was made, and little data was stored. Progressively, as managerial rationalism took hold, as labour became more efficient through specialisation, and as consumer marketing businesses became larger, more personal data came to be captured. During the second half of the twentieth century, enormous advances in information technology resulted in the capacity for marketers to depend more and more on data as a substitute for knowledge of their customers, and to become more and more remote from them.

But businesses can choose the appropriate degree of dependence on intensive personal data. They can enable anonymous and pseudonymous purchasing, by denying themselves the opportunity to consolidate data about each customer, to use it, and to pass it on to others. Even where they transact with known identities, they can limit the data that they retain (as some vendors do, for example, by not retaining credit-card details).

Businesses that hold identified data need to implement appropriate organisational security measures to protect it.

It was suggested in Clarke (1998) that direct marketing using electronic channels would be more successful if the following principles were applied:

- **Information** about the marketer's use of the technology should be readily available to anyone who seeks it, and sufficient to enable people to understand how it works, and what it entails;
- **Choice** should exist, such that each consumer can judge whether or not to engage in a relationship, or receive communications;
- **Consent** is needed from each consumer for the establishment of a relationship and the receipt of communications. Express consent is strongly preferable; but implied consent may be appropriate in a few circumstances. Consent requires an 'opt-in' arrangement, such that the person agrees in advance to the activity. 'Opt-out' arrangements may be cheap, but they are not consumer-friendly, and require stringent justification, of a kind that consumers will be comfortable with. This is discussed in greater detail in Clarke (2002b);
- **Fair Conditions** are important, such that each consumer has grounds for being confident in the nature of the commercial relationship;
- **Recourse** is a vital element, such that marketer behaviour that does not comply with these norms can be brought under control.

3.2 Technological Protections

Information technology has been primarily harmful to the privacy interest, resulting in increasingly widespread use of the term Privacy-Invasive Technologies, or 'the PITs' (Clarke 2001a).

A movement has been in train for a decade now, intended to apply information technology in support of privacy rather than against it. This goes under the name Privacy-Enhancing Technologies (PETs), a term which appears to have originated in IPCR (1995). See also EPIC (1996-) and Burkert (1997). Specialist PET Workshops have been held annually since 2001.

(Clarke 2001a) distinguishes three broad kinds of PETs:

- **PIT countermeasures, or counter-PITs**, designed to defeat or neutralise Privacy-Invasive Technologies. Examples include SSL/TLS for channel encryption, cookie managers, anti-spam measures and personal firewalls;
- **savage PETs**. These deny identity and provide genuine, untraceable anonymity. Examples include anonymous ('Mixmaster') remailers and web-surfing schemes, and David Chaum's payer-anonymous Digicash; and
- **gentle PETs**. Accountability is undermined by 'savage PETs', because retribution is difficult if the perpetrator cannot be identifed. Pseudonymity can provide a balance between the interests of privacy and accountability. But adoption is dependent on credibility, and pseudonymity is not credible if it can be readily circumvented by governments and corporations. Hence, as an alternative to Savage PETs, Gentle PETs are oriented towards protected pseudonymity.

3.3 Legal Protections

There are several heads of law which may provide privacy protections. The common law torts of confidence and passing off are of limited relevance in the present context. Those that are focussed on here are explicit data protection statutes, contract, and laws relating to misleading statements.

Since the first **data protection statute**, passed in 1970 in the German Land of Hesse, most 'advanced western' nations have enacted such laws. These all reflect the 'fair information practices' (FIPs) movement, which originated in American business and government circles in the late 1960s, but flowered in Europe during the 1970s (Flaherty 1989, Bennett 1992). FIPs was codified in the OECD Guidelines (1980).

The FIPs notion has proven to be utterly inadequate, with narrow scope, manifold exemptions and exceptions, and missing control mechanisms (Clarke 2000). Moreover, laws in most jurisdictions reflect the technology of the 1970s rather than that of the new century. FIPs has become so engrained, however, and the dominance of economic over social needs so strong, that the focus of public policy is very difficult to shift away from the nominal protection of data, back to the protection of people's privacy.

Almost alone among leading nations, the U.S. Congress has failed to enact comprehensive consumer privacy legislation. An exception is a statute relating to the privacy of children, the Children's Online Privacy Protection Act (COPPA). Such provisions are largely redundant in most countries with data protection laws, and COPPA is not a primary focus in this paper.

The U.S. Federal Trade Commission (FTC) has sought to roll back the protections that have emerged under the FIPs movement, by issuing its own, even more inadequate set of a mere four 'widely accepted fair information principles' – 'notice', 'choice', 'access' and 'security', to which it later added 'accountability' (FTC 2000).

This brought the U.S. into conflict with the E.U., because many U.S. consumer marketing corporations are active there. After a period of uncertainty, the E.U. chose to ignore the concerns of its advisory group (Art.29 2000), and backed down on key requirements. It permitted the U.S. to devise a so-called 'Safe Harbor' program (DOC 2000). This is an extension to the FTC's cut-down version of FIPs – with the original four principles supplemented by 'onward transfer', 'data integrity' and 'enforcement'; but despite the name of the principle, the scheme is not subject to effective enforcement.

Meanwhile, the U.S. Administration, through the Department of Commerce, has sought to undermine the OECD Guidelines by exerting its influence on members of the Asia-Pacific Economic Cooperation (APEC), in order to achieve publication of an alternative, much weaker set of principles (APEC 2004).

Contract law may also provide a basis for privacy protections. Vendors may offer explicit terms that the courts will treat as part of the contract binding vendor and consumer alike. Assurances about privacy protection may be embedded into those terms. Even where they are not, it is open to the courts, at least in common law jurisdictions, to find conditions to be implied in contracts. A PPS can form part of the terms of contract that the vendor and consumer enter into, either by the vendor's terms expressly reading in the PPS, or by the courts regarding the PPS as being an implied term of the contract.

The effectiveness of contract as a privacy protection is very limited, however. There is often vast disparity between the resources and market power of the parties, and the jurisdiction in which an action must be brought is often distant from and foreign to the consumer.

A further head of law of potential significance is provisions that make **misrepresentation** an illegal act. In common law countries, torts may exist that render misrepresentation a breach of the offended party's civil rights. Many countries have

created statutory obligations of a similar nature, and some recognise criminal misrepresentation. Examples include the U.K. Misrepresentation Act 1967, the Australian Trade Practices Act 1974 s.52, and Fair Trade Practices and Misrepresentation statutes in the various Australian States and Territories. Provided that the PPS takes the form of an undertaking by the vendor (rather than just a vague description or inherently untrustworthy advertisement), it is capable of being used as the basis for an action under such laws.

In the U.S., the Fair Trade Commission Act s.5(a) renders illegal an unfair or deceptive act or practice. This has been claimed to provide a similar restraint on privacy-abusive practices by American business (e.g. FTC 2005?). But the failure of the FTC to enforce under those provisions (having pursued only 15 cases in 7 years, in the world's largest and most dynamic economy) has shown the claims to be hollow. The FTC has even gutted the child protection law (the COPPA). It did this by determining that Amazon.com's Toy Store web site is "not directed at children" (EPIC 2004). Any organisation can now unilaterally declare itself outside the scope of the Act simply by stating that it "does not sell products for purchase by children".

The U.S. self-regulatory scheme has proven completely inadequate (Hoofnagle 2005), and is a much poorer deal for consumers than the inadequate FIPs-inspired laws in other countries. The longstanding calls for FIPs legislation (e.g. Clarke 1999a), which were temporarily quietened in the years immediately following the terrorist strikes of September 2001, have been resumed recently, with American business reported to be in support of regulation (Economist 2005).

PPS cannot directly protect privacy, in the way that organisational and technological measures can do so. They may, however, contribute indirectly to privacy protection, by providing evidence in support of legal actions, possibly for breach of contract, but more likely for misrepresentation.

4 Privacy Policy Statements

In the mid-to-late 1990s, it became fashionable in the U.S. for corporations to publish statements on their web-sites about their privacy practices (FTC 1998a, 1998b, Hoffman et al. 1999). This has been nominally encouraged by the relevant federal agency. In addition, the law of at least one U.S. State, California, imposes a requirement for a ‘privacy policy’ to be posted conspicuously by commercial web-site operators. See the California Business and Professions Code, ss. 22575-22579, which tools effect on 1 July 2004.

The notion has been adopted in other countries as well. In many countries it is primarily symbolic, because a data protection statute that regulates the private sector is far more likely to be effective than a mere statement by the organisation itself.

This paper adopts the view that, although a mere statement can only be a small part of a comprehensive approach to privacy protection and hence consumer trust in B2C eCommerce, there is nonetheless potential value in PPS. The reasons are as follows:

- publishing a PPS can motivate corporations to reflect their declared corporate privacy undertakings in their business processes;
- in countries that have data protection laws, publishing a PPS involves the articulation of corporations' legal responsibilities. The existence of a PPS may simplify complaints-handling and actions in tribunals and courts; and
- in those countries without effective data protection laws, such as the U.S.A., the existence of a PPS may provide a basis for actions possibly in contract or under misrepresentation laws, as a limited substitute for explicit statutory protections.

A variety of researchers have examined various aspects of web-site privacy statements. Foundation works included Culnan (1993) and Smith et al. (1996). Important among the analyses and empirical investigations have been Wang et al. (1998), Anton & Earp (2001), Earp et al. (2002), Lichtenstein et al. (2002), Milne & Culnan (2002), Earp & Baumer (2003), Lichtenstein et al. (2003), Culnan & Bies (2003), Jensen & Potts (2004), Gauzente (2004), McRobb & Rogerson (2004) and Kobsa & Teltzrow (2005).

Some of these include evaluations of PPS, but the norms against which the assessments have been performed have mostly been the limited requirements of U.S. law. Most recently, McRobb & Rogerson (2004) evaluated 113 PPS for reading ease, degree of structure, length, and the presence or absence of particular informational elements. This paper adds to the growing literature by piloting the evaluation of PPS against a comprehensive normative template.

Doubts have been expressed about the value of a PPS. For example, Regan (2001) noted how infrequently they were accessed. Many authors have drawn to attention their complexity, notably FTC (2000) and Culnan & Milne (2001). The recent report by Kobsa & Teltzrow (2005) concluded that "76% of users find privacy policies very important, and 55% stated that a privacy policy makes them more comfortable disclosing personal information. However, privacy statements today are usually written in a form that gives the impression that they are not really supposed to be read. And this is indeed not the case: whereas 73% of the respondents ... indicate having viewed web privacy statements in the past (and 26% of them claim to always read them), web site operators report that users hardly pay any attention to them". This conflict between the apparent importance of privacy and the limited use of privacy statements has been referred to as a "disconnect between public opinion and public behaviour" (Regan 2003).

This 'disconnect' reflects the highly situational nature of privacy. Most of the time, most consumers are only vaguely concerned about privacy, and lack the motivation to seek out and read carefully phrased, turgid 'legalese'. But even vague concerns represent an impediment to the adoption of eCommerce. Moreover, once an individual consumer's concerns are triggered, the person may easily become an active avoider of web-commerce. In response to the limited use of PPS by consumers, the concept of 'layered notices' has been developed "to provide an easy to read one-page summary of a company's online privacy practices while conforming to all regulatory requirements and giving links to full legal statements and other relevant information" (Fleischer 2005. See also Crompton 2004).

Only limited guidance is available in the literature as to what constitutes an appropriate form for a PPS. One important exception is the linked documents OECD (2000a and 2000b). The Committee of European Data Protection Commissioners, meeting as the EU's Article 29 Working Group on Data Protection, has been reported as having published guidelines on corporate privacy notices in late 2004 (e.g. Pruitt 2005). But a search on the Article 29 Committee's web-site failed to provide access to a copy. A preliminary document is visible on the site of the German Federal Data Protection Commissioner (ICDCP 2003).

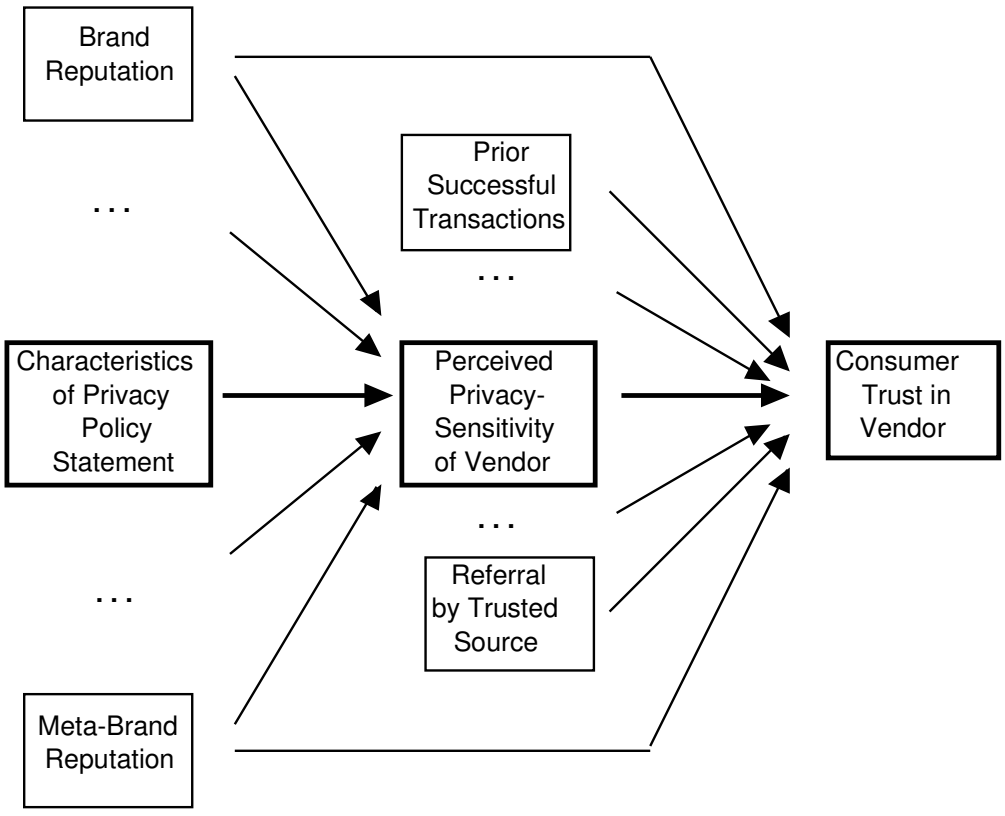
The web-sites of the various privacy protection agencies provide almost no assistance, although a publication of the U.K. Commissioner is of some relevance (ICO 2001). There are no guidelines apparent on the sites of the U.S. FTC, or even of the leading U.S. advocacy group EPIC and the more business-aligned groups CDT and EFF. Some guidance is provide by TRUSTe (2004 and 2005), and BBB (2003). But these documents are seriously limited, because they merely advise compliance with the FTC's minimalist FIPs model and a few U.S. sector-specific laws. Guidance intended for government agencies may also be of assistance, such as OFPC (2000?), AGIMO (2003) and TSB (2004).

As a prelude to the project reported on in this paper, this author drew on the above sources and his prior research, and compiled a Privacy Statement Template, at Clarke (2005a), with accompanying comments in Clarke (2005b). Both are readily accessible on the Web. That Template is applied in the research that is described below, as a basis for evaluating the PPS published by B2C vendors. The Template stipulates requirements in the areas of data collection, data security, data use, data disclosure, data retention and destruction, access by data subjects to personal data, information about data handling practices, the handling of enquiries, general concerns and complaints, enforcement, and changes to privacy undertakings.

5 Research Design

The research question being pursued is: 'How effective are Privacy Policy Statements in encouraging consumer trust of B2C vendors?'. The model that is assumed is as depicted in Exhibit 1.

Exhibit 1: Research Model



Consumer trust is heavily dependent on the vendor's perceived privacy sensitivity. That perception is in turn heavily dependent on the characteristics of the vendor's privacy policy statement. The purpose of the research is to consider the effectiveness of PPS from the perspective of the consumer. The research focusses on contexts in which vendors are seeking to implement substantive rather than merely image-based privacy

protections. It also leaves to one side the need for effective marketing communications, to ensure that consumers understand that the protections are in place.

The operational interpretation of the research question is: 'Do the Privacy Policy Statements found on vendors' web-sites measure up to the requirements expressed in the Privacy Statement Template'?

The vendor population is defined as those B2C services that are accessible on the World Wide Web. For simplicity, it does not encompass other forms of B2C eCommerce, such as emergent mobile services accessed through means other than web-browsers.

This is a highly diverse set of services. It is therefore important to analyse the population into meaningful segments, and probably important to over-sample from some of those segments. Exhibit 2 suggests a two-dimensional segmentation model that would appear to be appropriate to the research question.

For each segment, a sampling frame is needed. Examples include, for Market Leaders, businesses that receive frequent mentions in the media in relation to their privacy statements and terms of trade. For Aggressive Marketers, those organisations could be considered that have won awards for their B2C operations from such organisations as the (U.S.) Direct Marketing Association (DMA), or for whom Harvard case studies have been prepared. For Marketers of Sensitive Products, directories of on-line sex-shops and on-line gambling services could be consulted. Regional directories would provide links to marketers subject to the laws of particular jurisdictions. For 'Ethical' Marketers, directories of not-for-profit B2C operations, including charities, could be consulted.

Audit of the organisation's compliance with its PPS, and contact with the organisation to seek any clarifications, are both highly desirable. Such procedures are highly resource-intensive, however, and long delays and refusals might be anticipated. It is therefore envisaged that all judgements will be based on the PPS review, supplemented by experiments with the relevant service.

6 The Pilot Survey

A pilot survey was conducted. The primary purpose was to gain insight into the efficacy and practicability of the design, preparatory to its wider application. A secondary purpose was to gather information of relevance to policy discussions. The assessments were performed in January 2006.

6.1 The Sample

A small set of organisations was selected, in order to test the application of the Template to the PPS published by a manageably small list of organisations. These were selected in order to ensure some diversity, and to provide some prospect of results with some policy value. The organisations selected for evaluation are listed in Exhibit 3.

Company-Type	Description	Justification
Dimension 1 – The Company		Patterns in these categories may be materially different, because consumer trust is easier to achieve in an organisation with physical presence
A: 'Pure Internet' B2C	Corporations that do not have a separate physical operation	
B: 'Clicks and Mortar' B2C	Corporations that do have a separate physical operation	
Dimension 2– The Business		Patterns in these categories may be materially different, due to various characteristics of the business and its context
A: Leaders	Businesses acknowledged as trend-setters in this field	It would be valuable to over-sample this category, because it offers an indication of future directions
B: Aggressive Marketers	Businesses recognised as being strong and direct in their approach to consumers	These businesses could be expected to be either disdainful of privacy, or manipulative and image-conscious
C: Marketers of Sensitive Products	Businesses that sell goods and services whose purchasers are likely to be particularly concerned about privacy	These businesses could be expected to be highly subject to, and very well aware of, the need for effective privacy and visible privacy protections
D: Regional Marketers	Businesses primarily active in particular jurisdictions	Companies that are subject to data protection laws could be expected to adopt different approaches to those that are not subject to such laws
E: 'Ethical' / Not For Profit Marketers	Businesses run by organisations that espouse strong values in relation to privacy	These operations could be expected to have adopted positive approaches to privacy protection

Exhibit 2: Population Segmentation

- Leaders:
  - Amazon
  - Google
- Aggressive Marketers:
  - Sears, Roebuck and Co.
- Marketers of Sensitive Products:
  - Adultshop.com
- Regional Marketers:
  - Autoteile-Meile.de, an online supplier of tyres and automotive spare parts
- 'Ethical' Marketers:
  - National Geographic, which presents itself as "the largest nonprofit scientific and educational institution in the world"

Exhibit 3: Pilot B2C Businesses

The two market-leaders are very apparent from media and popular discussions. The choice of a German company was based partly on the fact that the country has the longest history of data protection laws, and partly on the pragmatic grounds that German is the only language other than English that the author can read, and that he has more familiarity with data protection laws in German-speaking countries than with those in other parts of Europe.

6.2 Results

This section provides a brief summary of the outcomes. The URL for the assessment sheets is provided in the Reference List, and the archived copies of the PPS that were evaluated are available from the author on request.

National Geographic and Google both implement the 'layered notice' notion by offering a 'highlights' page as well as a PPS. Google provides further PPS in respect of some of its services. The other organisations in the sample offer a single web-page, ranging from an equivalent 1-1/2 pages of A4 (Adultshop.com) to 4-6 pages (Amazon, Autoteile-Meile.de and National Geographic).

The analysis of the **Google** PPS was the subject of Clarke (2005c). This was used in a parallel project, published as Clarke (2006). That study identified serious shortfalls in many areas. These included the particular use of cookies, the vagueness of the statements about the purposes of the data Google collects, its transfer of personal data across borders, the absence of assurances about relevance and quality of personal data, its apparent attempt to obfuscate the meaning of 'consent', its failure to take any responsibility for personal data transferred to affiliates or to any other organisation, its failure to even address data retention and destruction issues, its failure to provide information about its data-handling processes, even on request, the general unenforceability of the assurances given, and the complete absence of protections in the event of merger, acquisition, or even sale of assets. In short, the several positive aspects of Google's PPS are completely swamped by very serious deficiencies.

Amazon has declared for itself extraordinary latitude in its handling of personal data. The effect of the statements is essentially that it collects personal data from wherever it wants to, uses it however it wants to, and discloses it to whomever it wants to. It provides minimal information on data security, none on data retention and destruction, little on amendment, and none on deletion of personal data. In common with other organisations, it provides no access to previous versions of its PPS. Amazon has previously changed its PPS, reneging on previous undertakings, and providing itself with additional latitude (e.g. Rosencrance 2000a, 2000b). It has also been accused of breaches of the Children's Online Privacy Protection Act (EPIC 2003), but the FTC found a way to ensure that the breach was only of the spirit rather than of the letter of the law (EPIC 2004).

Testing of the **Sears** site was made more difficult by its non-standard or bug-laden code, which caused malfunctions of the mainstream Mac Mozilla 1.7.8 browser being used. The PPS was found to have a wide array of deficiencies, not unlike Google's, but in some respects worse. For example, the concept of 'voluntary provision' of personal data was used in relation to data whose provision appears to be a condition of dealing; collection from and disclosure to third parties is undertaken on a non-consensual basis; the company appears to have no concept of data destruction on expiry of use; and no information is evident about any complaints process. This is consistent with a consumer-arrogant operation rather than a privacy-sensitive stance.

Adultshop.com is admittedly a very much smaller operation than the previous three, but its PPS is the antithesis of theirs. The page is expressly used as part of its positioning: "Our business success depends on our discretion and our understanding of the importance of your privacy. If you have suggestions for enhancing our privacy policy, please contact me directly ... Malcolm Day, Managing Director". All statements are directly expressed, and all options taken are privacy-sensitive. It falls short of the Template's requirements on many details (e.g. re data retention, access by the data subject, changes to the PPS, and acquisition, merger and sale of business). But many of these weaknesses are far less important because of the business process design. It is possible that the site's privacy-sensitivity reflects the fact that the organisation is subject to a data protection law (the Australian Privacy Act's private sector provisions, enacted in 2000). That is, however, a very weak implementation of the OECD FIPs model, and it is reasonable to infer that the copmany's perception of the needs of its customers was a significant factor in determining its approach.

The PPS published by **National Geographic** is remarkable in two ways:

- it is brutally frank about the vast array of data collection, use and disclosure techniques it uses; and
- it features a complete absence of choice ("If you do not agree to this Privacy Policy, please do not use this Web site").

The privacy terms are arguably far worse even than those of Sears, Roebuck and Co. They fail dismally in relation to all of data collection, security, use, disclosure, retention and destruction, personal access and complaints-handling. They impose opt-out where consent (opt-in) is the norm. They provide no means to communicate complaints to the company. Perhaps the PPS has been designed by a very clever lawyer so that it complies with the letter of the FTC's suggestions (although probably not with the additional requirements of the 'Safe Harbor' program). But it would appear to be non-compliant, at the very least with the basic choice and access principles, and the additional onward transfer and enforcement principles. Perhaps large U.S. not-for-profit organisations have become imbued with the aggressive ethos of American corporations. National Geographic was included in the pilot as a member of the 'ethical' segment, but its ethicality seems to be limited to honesty about the organisation's privacy-hostile stance.

The PPS of the German company, **Autoteile-Meile**, is subject to the German data protection law, the Bundesdatenschutzgesetz ss. 1-11 and 27-46. Remarkably, however, the document is to a very considerable extent a German translation of the current Amazon PPS (to the extent that it appears that it may be in breach of Amazon's copyright). It therefore inherits a large proportion of the weaknesses of that document. A number of modifications are apparent, to reflect the provisions of the German law. Others that might have been expected have not been made, however. It could be that the document is merely experimental, because it would seem to have little or no status under German law. Amazon has successfully opted out of the U.S. child privacy regulatory scheme merely by putting some well-chosen words on its web-site; but such corporation-friendly looseness is not a feature of European laws.

Observations arising from the pilot evaluations are as follows:

- there is a vast amount of internal integration among business units within business groups, and many corporations are making the assumption that individuals who transact with a business unit thereby provide their data to the entire group;
- the scale of inter-twining among 'independent' businesses is enormous. Major consumer marketing corporations appear to regard personal data as being theirs to share with any company they do business with, as they see fit;
- the inclusion in a business group of a popular search-engine (as is the case with both Google and Amazon) delivers a great deal of additional consumer profile information, in the form of search-terms;
- there is a tendency towards tempting individuals to provide data about other people into corporate databases. This is most evident in the social networking service, Google's Orkut. But the prospect exists of Amazon's Friends and Favorite People features being expanded;
- there is evidence that the self-permissive expressions used by American corporations (because of the substantial absence of a regulatory scheme there) are being adopted by companies elsewhere, even in circumstances in which the companies are subject to more stringent requirements.

One outcome of surprise was that it was not always as easy as it should be to discover the PPS. This identified the need to add an accessibility requirement into the Template. In most cases, the PPS was accessible from the home-page and from pages typically used during a consumer transaction. But Google does not have a link on its main pages at www.google.com, nor in country-specific services such as www.google.com.au nor even www.google.de. It is necessary to follow the link to 'About Google' to find the link. All of the others offer the link in the page-footer, and some also draw it to attention at a relevant point in the purchasing process.

Other **omissions from the template** that became apparent during the course of the evaluations were:

- the need for the Data Security category to include a declaration that access control is imposed, and that accesses are limited to individuals/roles with a demonstrated 'need to know' the particular information;
- the need for the Data Use category to include a requirement similar to that in the Data Disclosure category, to the effect that 'use is limited to those data-items necessary in the circumstances'.

Some doubt was thrown on the **segmentation** used in the research design. In particular:

- there may be a need for a further dimension of corporation size or scale of operation. The patterns of use and abuse of personal data vary a great deal, and are apparently significantly related to the size and complexity of business operations;
- there may be a need for a further dimension of jurisdiction(s) in which the organisation operates. The largely unfettered freedom in the U.S.A. is very distinct from the somewhat regulated environments in many other countries. A further consideration is that the virility of U.S. marketers is such that international consumer sales are showing a tendency towards globalism and hence the imposition of US. laissez faire on consumers everywhere, despite the protections they may enjoy in their own country.

7 Conclusions

In order to overcome consumer concerns about privacy-invasive practices in B2C eCommerce, there is no substitute for legal protection. Privacy policy statements originated within the U.S. 'self-regulatory' context, but are capable of playing a role within a statutory data protection framework as well.

A research design has been prepared, intended to enable evaluation of privacy policy statements against a normative template. A pilot survey applying the design to six organisations has established that the design requires refinement, but is largely appropriate.

To the extent that substantive conclusions can reasonably be drawn from the pilot survey, it appears that major American corporations, and even not-for-profits, may fall far short of the privacy-sensitive norms that consumers would reasonably expect in relation to the handling of personal data. More consumer-friendly practices appear to be associated with two factors: a statutory framework for data protection, and vendors of especially sensitive goods and services. These tentative inferences of course need to be tested through the evaluation of a larger, and more representative sample of privacy policy statements.

Complementary research is needed, to address aspects of the research question that were intentionally left to one side. In particular, studies are needed of the extent to which consumers understand the degree of privacy-protectiveness that they do and do not enjoy when using different companies' services, and the extent to which their adoption and non-adoption decisions reflect that understanding.

References

Except as otherwise noted, all URLs were most recently accessed 7-9 January 2006.

The detailed assessment sheets used in the PPS evaluations are at: http://www.anu.edu.au/people/Roger.Clarke/EC/PPS0601-Wrking.rtf

AGIMO (2003) 'The Guide to Minimum Website Standards – Attachment C: Privacy Checklist' Australian Government Information Management Office, Canberra, April 2003, http://www.agimo.gov.au/practice/mws/attachments#C

Ajzen I. & Fishbein M. (1980) 'Understanding Attitudes and Predicting Social Behavior' Prentice Hall, Inc., Englewood Cliffs, New Jersey, 1980

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

APEC (2004) 'APEC Privacy Framwework', Asia-Pacific Economic Council, November 2004, at http://203.127.220.112/content/apec/news___media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.downloadlinks.0001.LinkURL.Download.ver5.1.9

Art.29 (2000) 'Opinion 4/2000 on the level of protection provided by the 'Safe Harbor Principles'' Article 29 Data Protection Working Party of the European Union, 16 May 2000, at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2000/wp32en.pdf

BBB (2003) '', at https://www.bbbonline.org/privacy/sample_privacy.asp

Belanger F., Hiller J. & Smith W. (2002) 'Trustworthiness in electronic commerce: The role of privacy, security, and site attributes' J. Strat. Infor. Syst. 11, 3 & 4 (September & Dceember 2002) 245-270

Bennett C. (1992) 'Regulating Privacy: Data Protection and Public Policy in Europe and the United States' Cornell University Press, New York, 1992

Burkert H. (1997) 'Privacy-Enhancing Technologies: Typology, Critique, Vision' in Agre P.E. & Rotenberg M. (Eds.) (1997) 'Technology and Privacy: The New Landscape' MIT Press, 1997

Clarke R. (1998) 'Direct Marketing and Privacy' Xamax Consultancy Pty Ltd, February 1998, at http://www.anu.edu.au/people/Roger.Clarke/DV/DirectMkting.html

Clarke R. (1999a) 'Internet Privacy Concerns Confirm the Case for Intervention' Commun. ACM 42, 2 (February 1999) 60-67, at http://www.anu.edu.au/people/Roger.Clarke/DV/CACM99.html

Clarke R. (1999b) 'The Willingness of Net-Consumers to Pay: A Lack-of-Progress Report' Proc. 12th Int'l Bled Electronic Commerce Conf., Bled, Slovenia, June 7 - 9, 1999, at http://www.anu.edu.au/people/Roger.Clarke/EC/WillPay.html

Clarke R. (2000) 'Beyond the OECD Guidelines: Privacy Protection for the 21st Century' Xamax Consultancy Pty Ltd, January 2000, at http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html

Clarke R. (2001a) 'Introducing PITs and PETs: Technologies Affecting Privacy' Privacy Law & Policy Reporter 7, 9 (March 2001) 181-183, 188, at http://www.anu.edu.au/people/Roger.Clarke/DV/PITsPETs.html

Clarke R. (2001b) 'Meta-Brands' Privacy Law & Policy Reporter 7, 11 (May 2001), at http://www.anu.edu.au/people/Roger.Clarke/DV/MetaBrands.html

Clarke R. (2001c) 'Privacy as a Means of Engendering Trust in Cyberspace' UNSW L. J. 24, 1 (July 2001) 290-297, at http://www.anu.edu.au/people/Roger.Clarke/DV/eTrust.html

Clarke R. (2002a) 'Trust in the Context of e-Business' Internet Law Bulletin 4, 5 (February 2002) 56-59, at http://www.anu.edu.au/people/Roger.Clarke/EC/Trust.html

Clarke R. (2002b) 'e-Consent: A Critical Element of Trust in e-Business' Proc. 15th Bled Electronic Commerce Conference, Bled, Slovenia, 17-19 June 2002, at http://www.anu.edu.au/people/Roger.Clarke/EC/eConsent.html

Clarke R. (2005a) 'Privacy Statement Template' Xamax Consultancy Pty Ltd, December 2005, at http://www.anu.edu.au/people/Roger.Clarke/DV/PST.html

Clarke R. (2005b) 'About the Privacy Statement Template' Xamax Consultancy Pty Ltd, December 2005, at http://www.anu.edu.au/people/Roger.Clarke/DV/PSTA.html

Clarke R. (2005c) 'Evaluation of Google's Privacy Statement against the Privacy Statement Template of 19 December 2005' Xamax Consultancy Pty Ltd, December 2005, at http://www.anu.edu.au/people/Roger.Clarke/DV/PST-Google.html

Clarke R. (2006) 'Gurgle - The Turmoil Induced by a Search-Engine' Forthcoming in Computer Law & Security Report, at http://www.anu.edu.au/people/Roger.Clarke/II/Gurgle0512.html

Crompton M. (2004) 'Short Notices – why the Sydney resolution was adopted and progress in Australia since September 2003', Proc. 26th Int'l Conf. Privacy and Personal Data Protection, 14-16 September 2004, Wroclaw, Poland, at http://26konferencja.giodo.gov.pl/data/resources/CromptonM_paper.pdf

Culnan M. (1993) 'How Did They Get My Name? An Exploratory Investigation of Consumer Attitudes Towards Secondary Information Use' MIS Quarterly 17, 3 (September 1993) 341

Culnan M.J. & Milne G.R. (2001) 'The Culnan-Milne Survey on Consumers & Online Privacy Notices : Summary of Responses' Federal Trade Commission, 2001, at http://www.ftc.gov/bcp/workshops/glb/supporting/culnan-milne.pdf

Dinev T., Bellotto M., Hart P., Colautti C., Russo V. & Serra I. (2005) 'Internet Users, Privacy Concerns and Attitudes towards Government Surveillance - An Exploratory Study of Cross-Cultural Differences between Italy and the United States' Proc. 18th Int'l eCommerce Conf., Bled, June 2005, at http://aisel.isworld.org/pdf.asp?Vpath=BLED&PDFpath=41Dinev.pdf

DOC (2000) 'Safe Harbor Overview', U.S. Department of Commerce, 2000, at http://www.export.gov/safeharbor/sh_overview.html

Earp J.B. & Baumer D. (2003) 'Innovative Web Use To Learn About Consumer Behavior and Online Privacy' Commun. ACM 46, 4 (April 2003) 81-83

Earp J., Anton A. & Jarvinen O. (2002) 'A Social, Technical, and Legal Framework for Privacy Management and Policies' Proc. Americas Conf. on Information Systems 2002, at http://aisel.isworld.org/pdf.asp?Vpath=AMCIS/2002&PDFpath=021101.pdf

Economist (2005) 'Demon in the machine: Privacy laws gain support in America, after a year of huge violations' The Economist 1 December 2005, at http://www.economist.com/business/displayStory.cfm?story_id=5259499&no_na_tran=1

EPIC (1996-) 'EPIC Online Guide to Practical Privacy Tools', at http://www.epic.org/privacy/tools.html

EPIC (2003) 'EPIC Complaint and Request for Injunction, Investigation and for Other Relief In the Matter of Amazon.com, Inc.', Electronic Privacy Information Center, April 22, 2003, at http://www.epic.org/privacy/amazon/coppacomplaint.html

EPIC (2004) 'FTC Fails To Enforce Children's Privacy Law Against Amazon.Com' EPIC Alert 11.23, December 8, 2004, at http://www.epic.org/alert/EPIC_Alert_11.23.html

Flaherty D.H. (1989) 'Protecting Privacy in Surveillance Societies' Uni. of North Carolina Press, 1989

Fleischer P. (2005) 'Protecting Customer Data in an Evolving Technology Environment' Microsoft, 7 September 2005, at http://www.microsoft.com/emea/presscentre/peterfleischer.mspx

FTC (1998a) 'Privacy Online: A Report to Congress' Federal Trade Commission, June 1998, at http://www.ftc.gov/reports/privacy3/priv-23a.pdf

FTC (1998b) 'Self-Regulation Is The Preferred Method Of Protecting Consumers' Online Privacy' Federal Trade Commission, July 1998, at http://www.ftc.gov/opa/1998/07/privacyh.htm

FTC (1999) 'Protecting Consumers Online: A Federal Trade Commission Report on the First Five Years of Its Internet Law Enforcement Program' Federal Trade Commission, December 1999

FTC (2000) 'Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress' Federal Trade Commission, May 2000, at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf

FTC (2005?) 'Enforcing Privacy Promises: Section 5 of the FTC Act' Federal Trade Commission, 2005?, at http://www.ftc.gov/privacy/privacyinitiatives/promises.html

Gauzente C. (2004) 'Web Merchants' Privacy And Security Statements: How Reassuring Are They For Consumers? A Two-Sided Approach' J. of Electronic Commerce Research, 5, 3 (2004), at http://www.csulb.edu/web/journals/jecr/issues/20043/Paper4.pdf

Hoffman D.L., Novak T.P. & Peralta M. (1999) 'Building Consumer Trust Online' Commun. ACM 42, 4 (April 1999) 80-85

Hoofnagle C. J. (2005) 'Privacy Self Regulation: A Decade of Disappointment' Electronic Privacy Information Center, March 4, 2005, at http://www.epic.org/reports/decadedisappoint.html

ICDCP (2003) 'Proposed Resolution on Improving the Communication of Data Protection and Privacy Information Practices' Proc. 25th International Conference Of Data Protection & Privacy Commissioners Sydney, 12 September 2003, at http://www.bfdi.bund.de/cln_030/nn_535764/SharedDocs/Publikationen/EN/InternationalDS/ConferenceOfInternationalDataProtectionCommissioners2003ResolutionOnImprovingTheCommunicationOfDataProtectionAndPrivacyInformationPractices.html

ICO (2001) 'Compliance advice: Website Frequently asked questions' Information Commissioner's Office, Manchester, U.K., 26 June 2001, at http://www.ico.gov.uk/documentUploads/Website%20FAQ.pdf

IPCR (1995) 'Privacy-Enhancing Technologies: The Path to Anonymity' Information and Privacy Commissioner (Ontario, Canada) and Registratiekamer (The Netherlands), 2 vols., August 1995, at http://www.ipc.on.ca/web%5Fsite.eng/matters/sum%5Fpap/papers/anon%2De.htm

Lee M.K.O. & Turban E. (2001) 'A Trust Model for Consumer Internet Shopping' Int'l J. of Electronic Commerce 6, 1 (September 2001) 75-91

Jensen C. & Potts C. (2004) 'Privacy Polices as Decision-Making Tools: An Evaluation of Privacy Notices' Proc. CHI 2004, April 24-29, 2004, Vienna, Austria

Kim D. (2005) 'Cognition-Based Versus Affect-Based Trust Determinants in E-Commerce: Cross-Cultural Comparison Study' Proc. Int'l Conf. on Information Systems, 2005, at http://aisel.isworld.org/pdf.asp?Vpath=ICIS/2005&PDFpath=WBISA03.pdf

Kobsa A. & Teltzrow M. (2005) 'Impacts of Contextualized Communication of Privacy Practices and Personalization Benefits on Purchase Behavior and Perceived

Quality of Recommendation' Proc. Workshop: Beyond Personalization 2005 IUI'05, January 9, 2005, San Diego, California, USA, at http://www.cs.umn.edu/Research/GroupLens/beyond2005

Lichtenstein, S., Swatman, P.M.C. and Babu, K. (2002) "Effective Online Privacy Policies" In Information Systems: Enabling Organisations and Society: Proceedings of Thirteenth Australasian Conference on Information Systems, Victoria University, Melbourne, Australia

Lichtenstein, S., Swatman, P.M.C & Babu, K. (2003) "Narrowing the Gap Between Privacy Policy and Practice: Guidelines and Framework for Integrating Online Privacy Policy With Practice", Working Paper 2003/05, School of Information Systems, Deakin University, Melbourne, Australia

McRobb S. & Rogerson S. (2004) 'Are they really listening? An investigation into published online privacy policies at the beginning of the third millennium' Infor. Techno. & People 17, 4 (December 2004) 442-461

Milne G.R. & Culnan M. J. (2002) 'Using the content of online privacy notices to inform public policy: a longitudinal analysis of the 1998-2001 U.S. web surveys' The Information Society 18, 5 (October 2002) 345-359

OECD (1980) 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' Organisation for Economic Cooperation and Development, Paris, 1980, at http://www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html

OECD (2000a) 'Developing a Privacy Policy and Statement' Organisation for Economic Co-operation and Development, Paris, 2000, at http://www.oecd.org/document/1/0,2340,en_2649_34255_28863233_1_1_1_1,00.html

OECD (2000b) 'OECD Privacy Statement Generator' Organisation for Economic Co-operation and Development, Paris, 2000, at http://www.oecd.org/document/39/0,2340,en_2649_34255_28863271_1_1_1_1,00.html

OFPC (2000?) 'Guidelines for Federal and ACT Government Websites' Office of the Federal Privacy Commissioner, Sydney, Australia, undated, at http://www.privacy.gov.au/internet/web/index.html

Palmer J.W., Bailey J.P. & Faraj S. (2000) 'The Role of Intermediaries in the Development of Trust in the WWW: The Use and Prominence of Trusted Third Parties and Privacy Statements' J. of Computer-Mediated Communication 5, 3 (March 2000)

Pruitt S. (2005) 'Europe takes lead on improving online privacy notices' The Industry Standard, 4 April 2005, at http://www.thestandard.com/internetnews/002774.php

Regan K. (2001) 'Does Anyone Read Online Privacy Policies?' E-Commerce Times, 15 June 2001, at http://www.ecommercetimes.com/story/11303.html

Regan P. (2003) 'Privacy and Commercial Use of Personal Data: Policy Developments in the United States' J. of Contingencies and Crisis Management 11, 1 (March 2003) 12-18

Rosencrance L. (2000a) 'Amazon Loses 2 Partners Over Privacy Policy' Computerworld, September 18, 2000, at http://www.computerworld.com/cwi/story/0,1199,NAV47_STO50529,00.html

Rosencrance L. (2000b) 'Amazon.com's Privacy Policies in Spotlight Again, U.S., U.K. Probes Urged' Computerworld, December 11, 2000, at http://www.computerworld.com/cwi/story/ 0,1199,NAV47_STO54993,00.html

Smith H.J., Milberg S.J. & Burke S.J. (1996) 'Information Privacy: Measuring Individuals' Concerns About Organizational Practices' MIS Qtly 20, 2 (June, 1996)

TSB (2004) 'Directive on Government of Canada Web Site privacy policies' Treasury Board of Canada Secretariat, Ottawa, 5 November 2004, at http://www.tbs-sct.gc.ca/gos-sog/impl-rep/impl-rep2000/imp.report71/att-pj_e.htm

Truste (2004) 'Your Online Privacy Policy', Truste, 2004, at http://www.truste.org/pdf/WriteAGreatPrivacyPolicy.pdf

Truste (2005) 'TRUSTe Guidance on Model Web Site Disclosures' Truste, August 2005, at http://www.truste.org/docs/Model_Privacy_Policy_Disclosures.doc

Wang H., Lee M.K.O. & Wang C. (1998) 'Consumer privacy concerns about Internet marketing' Commun. ACM 41, 3 (March 1998) 63 - 70

Xu Y., Tan B, Hui K-L. & Tang W-K. (2003) 'Consumer Trust and Online Information Privacy' Proc. Int'l Conf. on Information Systems, 2003, at http://aisel.isworld.org/pdf.asp?Vpath=ICIS/2003&PDFpath=03CRP45.pdf