

---

## **Privacy as a shared feature of the e-phenomenon: a comparison of privacy policies in e-government, e-commerce and e-teaching**

---

Steve McRobb\* and Bernd Carsten Stahl

Centre for Computing and Social Responsibility  
De Montfort University  
The Gateway, Leicester LE1 9BH, UK  
E-mail: smcrobbs@dmu.ac.uk  
E-mail: bstahl@dmu.ac.uk  
\*Corresponding author

**Abstract:** One of the characteristics shared by most, if not all, aspects of the e-phenomenon is that it poses new challenges to privacy. This paper will discuss the concept of privacy and analyse which differences regarding the attention to privacy exist between different sectors. Based on a broad literature review on the ethical foundations of privacy, we have identified three research questions:

- 1 What are the reasons given by organisations to protect privacy?
- 2 What is the perceived nature of privacy?
- 3 How do organisations address different stakeholders?

These questions are explored by analysing the privacy policies of organisations from three different sectors: e-commerce, e-teaching and e-government. We will argue that the three sectors come to different answers to the above questions but that privacy is an overarching concern that needs to be addressed. It is therefore justified to say that the e-phenomenon exists, at least in so far as it creates a necessity for organisations to consider the issues raised by privacy.

**Keywords:** e-commerce; e-teaching; e-government; privacy; privacy policy.

**Reference** to this paper should be made as follows: McRobb, S. and Stahl, B.C. (2007) 'Privacy as a shared feature of the e-phenomenon: a comparison of privacy policies in e-government, e-commerce and e-teaching', *Int. J. Information Technology and Management*, Vol. 6, Nos. 2/3/4, pp.232–249.

**Biographical notes:** Steve McRobb is a Senior Lecturer in Information Systems at De Montfort University, UK. He is co-author of a successful textbook on Object-Oriented Systems Analysis and Design and an Associate Researcher with the Centre for Computing and Social Responsibility. His current research interests are in privacy online and the effects of ICT on power and trust. McRobb was formerly Principal Administrative Officer at the Yorkshire Dales National Park. For more information, see <http://www.cse.dmu.ac.uk/~smcrobbs/>.

Bernd Carsten Stahl is a Reader in Critical Research in Technology of the School of Computing and a Research Associate at the Centre for Computing and Social Responsibility of De Montfort University, Leicester, UK. His interests cover philosophical issues arising from the intersections of business, technology, and information. This includes the ethics of computing and critical

approaches to information systems. He is the Editor-in-Chief of the *International Journal of Technology and Human Interaction*. More information can be found under: <http://www.cse.dmu.ac.uk/~bstahl/>.

---

## **1 Introduction**

Like most large and distributed phenomena, the e-phenomenon is difficult to grasp and define. One can argue that it is not a single phenomenon but a collection of disparate, even dissimilar, occurrences. On the other hand, the 'e-' prefix has gained currency and seems to mean something to many people. In this paper we will not contribute to the metaphysical discussion about whether there is an 'essence' behind the phenomena or whether it is justified to even talk about a single phenomenon. Rather, we will examine three aspects of the e-phenomenon, namely e-commerce, e-government and e-teaching, and identify a problem they all share: privacy. In all three areas, the problem of the protection of individual data has become important, albeit on different grounds and with different implications. We will argue in this paper that privacy currently is, and will most likely remain, a central issue in e-enabled interaction and that a failure to consider it in depth may lead to the failure of the e-phenomenon.

The paper starts with a brief review of the literature on e-commerce, e-government and e-teaching, concentrating on the way the issue of privacy is framed and addressed. On the basis of this analysis, we will proceed to discuss our empirical research. We have analysed privacy policies from all three areas and will present the findings of this analysis. Our approach builds upon previous empirical enquiries into the content and characteristics of online privacy policies (for example, Johnson-Page and Thatcher, 2001; Milne and Culnan, 2002; Desai *et al.*, 2003; Gauzente, 2004; McRobb and Rogerson, 2004a–b; 2005).

## **2 The concept of privacy**

The term 'privacy' has come to be used ubiquitously, but its meaning becomes less clear when one tries to pin it down. We collectively value it, but there seems little agreement on why we do so (Weckert and Adeney, 1997). We can ask whether it refers to a situation, a right, a claim, a form of control, or a value (Gavison, 1995). We can organise a discussion of privacy by distinguishing between confidentiality, anonymity and data protection (Rotenberg, 1998), or according to the individuals whose data is involved, or according to the organisational environment in which it is discussed (Greenaway and Chan, 2005).

Concerns for privacy are very topical in an electronically enabled environment, but they are not new. They are found in some of the earliest texts of western civilisation and played an important role in ancient Greek democracy (Arendt, 1958). In modern Western society, privacy has had explicit legal standing for only a century (Sipior and Ward, 1995). An important reason why privacy has gained importance is the development of technology. The seminal definition of privacy as the 'right to be let alone' (Warren and Brandeis, 1890) was a reaction to the new technology of photography, which, for the first

time in history, allowed the detailed depiction of someone without that person's knowledge or agreement. Warren and Brandeis's definition is still widely used (Britz, 1999; Velasquez, 1998) even though it lacks clarity and applicability.

Rather than attempt a complete and comprehensive definition of privacy, it may be more promising to describe some of its important characteristics. One is that privacy has to do with control over personal information. It has been defined as "ability for an individual to control the use of their own personal data, wherever it might be recorded" (Fleming, 2003, p.128). This is problematic because in modern societies we have little control over information concerning ourselves (Tavani and Moor, 2001). However, the control aspect is important because it can be used to represent the widespread view that an invasion of privacy occurs when we are no longer able to control our interactions (Culnan, 1993). It also reflects the fact that we typically are not opposed to all sharing of information about ourselves, but that we wish to be in control of it. This allows a distinction between legitimate voluntary and problematic non-voluntary disclosure (Elgesem, 2001). The information control characteristic is closely linked with the idea of privacy as informational self-determination (Stalder, 2002), which in some European countries, notably Germany, has been recognised as a constitutional right.

A very different approach to privacy is that of (intellectual) property. This aims at the same goal, namely regulating access to personal information. But instead of concentrating on the question of who gets to control access according to which criteria, the argument links privacy with the well-established mechanisms of intellectual property. The argument basically states that everyone owns the information about himself/herself and that therefore access to such information can be regulated through the regulations of access to property (Spinello, 2000).

### 2.1 *Reasons for the defence of privacy*

If we want to understand the different reactions to the challenge of privacy in areas such as e-commerce, e-teaching and e-government, then we must understand why people value privacy. One can distinguish between arguments that concentrate on the importance of privacy for the individual and those that are centred on its organisational/social effects.

Breaches of privacy can be seen as problematic because they objectivise the other, because they render her a pure object of data collection (cf. Elgesiem, 1996). This is ethically problematic from a Kantian viewpoint, since the Categorical Imperative states that one should always treat the other as an end in himself, never as a pure means. It is also problematic from an existentialist perspective because it signals a lack of respect for the 'Other'. It can thus be argued to be bad *per se*, without any regard to possible consequences (Introna, 2003).

Such arguments are often not easily appreciated in the Anglo-American world, with its strong roots in utilitarianism and consequentialism. Here, we can distinguish between intrinsic versus instrumental value arguments (Spinello, 2000; Tavani, 2000; Moor, 2000). If privacy has intrinsic value, then it needs to be protected for its own sake. If it is instrumental, then privacy is to be valued for a higher good that it protects or promotes. Viewing privacy as an intrinsic value means that there is no need for its further justification; it needs to be protected. It thus takes on a status similar to a human right, which we typically do not defend with consequentialist arguments. Indeed, privacy is recognised as a human right, for example in Article 8 of the European Convention of Human Rights.

There are also a number of instrumental supports for privacy protection. These promote the protection of privacy because it serves some other good. On an individual level a minimum level of privacy protection seems to be required for humans to develop their potential. A lack of privacy can lead to defects in psychological health (Nissenbaum, 2001). It can lead to problems in developing the (moral) autonomy required for people to flourish (van den Hoeven, 2001). Protecting privacy can also be seen as an aspect of the right to freedom, which, in turn, is required to be able to enjoy one's other basic freedoms (Brey, 2001). Part of this argument is that privacy is important for forming personal identity (Severson, 1997; Brown, 2000; Nye, 2002). Another is that a lack of privacy and resulting problems of identity can lead to difficulties in building trusting relationships between individuals (Johnson, 2001; Gallivan and Depledge, 2003).

Individual considerations spill over into organisational and societal issues. If there is a lack of privacy and individuals do not develop to their full potential, then this is problematic on an aggregate level. A lack of privacy can thus jeopardise social interaction (Introna, 2000). An important aspect of the social relation issue is power, which has to do with the relationship between privacy and surveillance, and their impact on social interaction. A central concept here is the 'Panopticon'. Originally developed by Bentham, the idea was taken up by Foucault (1975). Bentham's idea was to arrange the cells of prison inmates in such a way that they could always be observed, but to leave it uncertain whether each individual was observed. He hoped this would lead the inmates to discipline themselves, a thought that Foucault followed to its unpalatable consequences. For our discussion, the Panopticon is relevant because it works by disregarding considerations of privacy. It has captured the imagination of IS/IT scholars and practitioners because new technologies arguably have the potential to realise a Panopticon by instituting electronic surveillance (Yoon, 1996; Robison, 2000; Goold, 2003).

Another social problem is that lack of privacy can hinder democratic participation. Democracy is rooted in the concept of an autonomous individual who is capable of subordinating herself to the preferences of the majority. This implies that individuals must have a private place of their own where they can withdraw from public interaction. Moreover, democratic practices explicitly realise that citizens may not want to make all of their thoughts known. This explains why we think elections have to be secret (Johnson, 2001; Gavison, 1995).

On an organisational level privacy may be desirable because it furthers organisational goals. Privacy considerations are important with regard to employer-employee relationships, organisational trust and employee work satisfaction. Taking employee privacy away, for example by instituting electronic surveillance, can hurt work relationships. It signals that management wants to exert strong control (Weisband and Reinig, 1995) and does not trust employees (Urbaczewski and Jessup, 2002).

## *2.2 Limits of privacy*

It is probably safe to say that a substantial percentage of organisations use some technology to gather data on individuals who are of interest to them. But it is important to note that, despite the good reasons for the protection of privacy, there are also good reasons to collect data and thereby possibly to jeopardise privacy.

We will discuss the specific motivations for organisations to collect data in the following section. First, it is useful to point out that there is a general acceptance that collecting personal information and breaching privacy is sometimes legitimate and may even be the only lawful and/or moral course of action. A simple thought experiment shows that this is the case. Let us assume that we lived in a world where there was complete privacy, which means that there would be no exchange of personal information. Such a world would clearly not work. We need to exchange information about ourselves in order to interact and to keep the community alive. But even a world where privacy was limited to organisations, *i.e.*, where personal information could be exchanged between individuals but not given to any sort of organisation, is not feasible. We could not exchange goods through organisations; there would be no state, no schools and no hospitals. It is thus obvious that privacy concerns can be overridden by other goods (cf. Rogerson, 1998). The question is what those goods are and why they are more important than privacy. The resulting question, which is at the heart of our paper, is: how do organisations deal with this question and how do they communicate their answers?

### **3 Privacy in different aspects of the e-phenomenon**

In this section we will briefly discuss the three aspects of the e-phenomenon we have chosen, namely e-commerce, e-teaching and e-government. For each area, we will briefly discuss the various arguments for and against privacy protection. This will lay the groundwork for understanding the different privacy policies of the three sectors.

#### *3.1 Privacy in e-commerce*

There have been many definitions of e-commerce, ranging from the simple and imprecise to the complex and comprehensive. One example from the latter end of the spectrum is given by the UK Cabinet Office Innovation and Performance Unit, which defines e-commerce as “exchange of information across electronic networks, at any stage in the supply chain, whether within an organisation, between businesses, between businesses and consumers, or between the public and private sectors, whether paid or unpaid” (Cabinet Office, 1999). This seems helpful, since it recognises that e-commerce is not just about money, but that the exchange of information is often its very essence. However, it is too broad for our purposes since it could include both e-teaching and e-government, which we wish to treat separately for reasons discussed earlier. Instead, we will adopt this definition from Wikipedia.org: “e-commerce... consists primarily of the distributing, buying, selling, marketing, and servicing of products or services over electronic systems such as the Internet and other computer networks”. This definition focuses on transactions with a commercial motivation, although the specific transaction may not involve the exchange of money. It also focuses implicitly on transactions between entities that have a commercial relationship involving the sale of goods and services. This can be argued to include internal relationships, such as employment, since these are typically based on the sale of one person’s services to another. Theoretical issues relating to both internal and external transactions are discussed below. But for simplicity’s sake, in the empirical research we will concentrate at this stage only on the external relationships of e-commerce; that is, those between a business and its customers.

Privacy issues have long been discussed in e-commerce. A considerable part of the literature reviewed above refers directly or indirectly to the application of e-commerce. Within e-commerce, there are privacy issues of customers and of employees, and the reasons for collecting data on those two groups can be very different. The combining feature is that they all have to do with making or retaining money.

With regard to employee privacy, companies may believe that misuse of technology costs them money by wasting time and productivity, or they may wish to forestall litigation arising from employees' misuse of technology (Straub and Collins, 1990). But the area of employee surveillance is complex (cf. Stahl *et al.*, 2005) and we cannot do it justice here. Our main interest is in privacy policies published on companies' websites, and these are chiefly aimed at customers and other external stakeholders.

Companies wish to collect data on customers and clients for many reasons. In particular, knowing one's customers can help to provide better products and services, create longer-term relationships and thereby maximise profits in the long run. It thus seems to be in the interest of companies to maximise the amount of data they can collect on customers. This would allow them to detect individual preferences and trends and to determine future avenues of activity. Strategic decision-making depends on understanding one's market and customers (Mason, 1986).

There are thus strong economic incentives to collect data on customers. However, customers are reluctant to give personal information above and beyond what is strictly necessary for economic interaction. Especially in e-commerce, buyers often do not know the company they are transacting with. There is no prior history which would allow them to develop trust, and they have little reason to provide personal data that may be used for purposes that are not beneficial to them. There are many examples of data collected for commercial purposes being used for other purposes than those initially stated. The challenge for commercial organisations is thus to persuade customers to provide the maximum amount of personal data that is useful for economic purposes, and at the same time not to appear unduly curious and thus raise customers' suspicion. For the company the question is thus one of profit maximisation. Their profit function will be at a maximum somewhere between the extremes of gathering no data and gathering all available personal information. Where this maximum lies is difficult to determine, and depends on culture, industry, products, legal environment and many other aspects.

### 3.2 *Privacy in e-government*

E-government can be defined as the application of electronic technology, especially the internet, to the purposes of government. Currently, it aims mostly at the provision of governmental services online, but has the more radical potential to change the participation of citizens in public decision-making. It may be useful to distinguish between these two aspects by using the terms 'e-government' and 'e-democracy' (Stahl, 2005). These two concepts and their practical implications are vastly different, but they can still be usefully contrasted with commercial activities. The transactions of e-government are in their technicalities very similar to those of e-commerce, and will often involve an element of payment. But they are carried out for very different motives, and we can expect this to be reflected in the nature of the concern for privacy. Companies are interested in privacy because it can affect their profits, while governmental organisations have a completely different interest. The Big Brother state was long the

main fear of civil libertarians and it seemed that the main threat to privacy came from governments who wanted to subdue their subjects. This theme of the debate changed with the apparent victory of democracy over totalitarianism at the end of the cold war. In the 1990s, the rise of e-commerce combined with the increasing ease and decreasing cost of processing information seemed to make businesses the main threat to privacy (cf. Himanen, 2001; Tavani, 2000; Castells, 1997). This change of roles currently seems to be reversing due to international concerns about terror and security.

This leads us to the reason why governments are seen as a danger to privacy. In principle democratic governments, which represent the will of the people, should act according to the people's preferences and, if privacy is a preference, should respect it. (We leave aside non-democratic governments, whose agendas are obviously opposed to privacy protection). Privacy, as we saw earlier, is at least related to some human rights and should therefore enjoy strong protection by governments.

The main problem with this sort of argument is that privacy can also be opposed to other interests of the state, most notably security. The relationship between privacy and security is complex (cf. Stahl, 2004), but when governments are able to combine information from a variety of databases and to data-mine huge amounts of information in a search for patterns, for example of terrorism, privacy can be seen as an impediment to such technology and thus to security.

Another issue is that it seems to be the nature of all systems of power to extend their reach. Western democracies therefore work with systems of checks and balances which limit the expansion of state power. Privacy is clearly one limit of state power because it protects information that states would have an interest in for a variety of reasons. Not only could states catch criminals, they could also widen their tax base, improve their statistics for decision-making or promote desired behaviour. This function creep is feared in countries with a strong liberal tradition, notably in the USA, which probably explains why privacy protection there is predominantly aimed at the state (Culnan, 1993).

With regard to the reason for displaying attitudes about privacy, one can assume that e-government will fundamentally differ from e-commerce. E-commerce is interested in economic gain but democratic governments are interested in the public good. They may misinterpret it or they may do a bad job, but a democratic government must cater to its constituencies and therefore take into account the views of the majority. E-commerce has a clear conflict of interest between those who collect data and those who display it, while e-government locates the conflict of interest elsewhere. The same people are interested in having their privacy protected and in limiting privacy for reasons of security. Where e-commerce must comply with legal regimes, governments create these and therefore must consider the question of legitimation more deeply. In this context, privacy is only one value in a plethora of competing values, which includes security but also others that must be balanced (cf. van den Hoven, 1999).

### 3.3 *Privacy in e-teaching*

E-teaching is an interesting field that, in some respects, lies between the two discussed above and, in other respects, is independent of both. We can define e-teaching as the use of electronic technology for the purposes of delivering education. This is another rather wide definition because a range of different applications exist from primary to secondary level, and also in further/higher education. It may mean the use of technology to support

a traditional delivery of education, or it may mean its reengineering. E-teaching can stand for on-site classroom education or for online distance education. Detailed discussion of such a wide field requires more space than we can give it here (cf. Leidner and Jarvenpaa, 1995; Alavi and Leidner, 2001; Piccoli *et al.*, 2001).

E-teaching is interesting because it is to some degree simultaneously an aspect of e-commerce and of e-government. On the one hand, education in general is a market and the e-enabled part of this market is huge and growing. In the USA, for example, the vast majority of Association to Advance Collegiate Schools of Business (AACSB) accredited business schools have some e-teaching provision in their portfolio (Tress, 2000). The market for e-teaching technology, consulting and other services is predicted to grow quickly (Huynh *et al.*, 2003).

On the other hand, e-teaching is often largely in the hands of the state. States tend to take responsibility for primary and secondary education and at least parts of further and higher education. This leads to a variety of stakeholders with very different interests with respect to privacy. One can distinguish at least between (commercial) providers, staff, students, educational institutions and sponsors (usually governmental). Some stakeholders have dual roles. Staff (teachers, lecturers), for example, are customers, but also citizens, and additionally they have a responsibility for teaching. Similarly, students are consumers but also citizens and in their student roles have diverging interests.

Let us consider a widespread example: a university uses a Virtual Learning Environment (VLE) to transmit teaching content to students. This automatically captures a variety of data on students and staff. The vendor has an interest in access to data to improve the system and to retain the university as a customer. Students require some of this information for their work but it can also render them more transparent for evaluation purposes. Staff will be forced to provide information and can also collect information, say, on student participation. At the same time, the university can easily check staff interaction with the system. The university has an interest in usage data and the sponsor will be interested to see whether the educational outcome is positive and whether the investment was worthwhile. On top of this, there are considerations of how additional data captured by a system can impact the relationships between the stakeholders, for example between staff and students or between staff and the university (Klein and Huynh, 2004).

Considerations of privacy are therefore different in an educational setting. There are other means of collecting data and other types of data of interest. More importantly, the mix of stakeholders and their interests will diverge. Privacy will nevertheless still be a central concern, and one that schools, colleges and universities can be expected to deal with explicitly when communicating with their stakeholders.

We can thus state that privacy appears to be a common issue in the different manifestations of the e-phenomenon. In the following section we will describe research which aimed to identify how organisations from the different sectors signal their approach to privacy. We will use these observations to investigate whether there are commonalities which would allow us to speak of privacy concerns as an overarching constituent of the different aspects of the e-phenomenon.

## **4 Privacy policies: an empirical comparison of the different areas**

### *4.1 Methodology*

The approach taken in this phase of our research has three main steps. First, we make some predictions, based on the earlier theoretical discussion, regarding how we expect the concept to be operationalised in the separate domains of e-commerce, e-government and e-teaching. Second, we conduct a limited empirical survey by collecting a small sample of typical privacy policy documents. These allow us to examine the extent to which our predictions are met in practice. Finally, the text of the privacy policy documents is interpreted for evidence that the privacy concerns are present (or not) as expected.

Earlier research indicates this is a rich and complex field that is not readily susceptible to simple quantitative methods (McRobb and Rogerson, 2004a–b; 2005). Thus our empirical approach is both qualitative and interpretive. We sought to discern the intentions and attitudes of some typical online organisations through a close reading of their policies. This differs from (while being related to) privacy practice, but attitude and intention are important factors that contribute to behaviour, and worthy of study in their own right.

We examined published online privacy policies of six organisations, two from each domain. Within each pair, one was from the UK and one from the USA. The e-commerce and e-government organisations were taken from a much larger sample that has been surveyed three times for a continuing longitudinal study (McRobb and Rogerson, 2004a–b; 2005). Two educational institutions were added to this sample specifically for this research.

Our approach is modelled on the larger study in that it combines a purposive sampling approach to data collection with an interpretive approach to its analysis. Purposive (or non-probability) sampling was adopted for the reason that (as will become clear from the theoretical discussion that follows) there is no real prospect of deriving from the findings results that could be generalised in a statistically valid way. The characteristics that we are interested in examining (statements taken to express underlying philosophical attitudes) are not readily reduced to objectively quantifiable variables.

We are interested in what each policy reveals about the attitudes and assumptions of its authors and editors. Therefore we chose to analyse a small number of policies for each domain, but not to attempt spurious tests of statistical significance. Although such an approach restricts the generality of the results, we do not believe this weakens our conclusions. The phenomena under examination are largely subjective in nature, and would not in any case support probabilistic deductions. But they are nevertheless important to understanding some social and cultural aspects of the wider e-phenomenon.

### *4.2 Research questions*

We examined policies in light of the following questions, which are derived directly from the theoretical considerations outlined earlier.

First, does the policy suggest a preference for the view that privacy is primarily important for intrinsic or for consequentialist reasons? In the e-commerce domain, we expected privacy considerations to be driven mainly by consequentialist reasoning,

ultimately reducible to profit maximisation. In relation to e-government, we expected that consequentialist reasons would play less of a role, and that the motivation is more likely to rest on intrinsic foundations. Educational institutions display some characteristics of the two other domains, so we expected the conceptual basis of privacy here to be more mixed.

Second, does the policy suggest a preference for considering privacy from a control, or from an ownership perspective, or both? There is a *prima facie* assumption that commerce, being built on ownership and private property, will rely on the construct of ownership, whereas governmental agencies are less interested in property but more in exerting control to fulfil their tasks.

Third, does the policy suggest that the organisation treats the privacy concerns of different stakeholders in different ways? And if so, are the different approaches appropriate to the interests and concerns of the group? Since the stakeholders vary between domains, but may be expected to be relatively homogenous within each domain, it seems reasonable to expect that this will be addressed in some way by the policies.

#### *4.3 Policies in the domain of e-commerce*

We selected Argos Limited from the UK and AT&T from the USA to represent this domain. Both are sizeable, well-established businesses with some maturity based on several years' experience in the field of e-commerce.

Although relatively clear and readable, the tone of the Argos privacy policy resembles that of a legal agreement. It begins with legal definitions and then states that the purpose of the policy is 'to set out how we may use personal information that we may obtain about you'. It indicates that, by using the website, and in particular by registering to use a service, the visitor consents to the use of his/her personal information as stated. This defensive posture suggests that one intention of the publishers is to give Argos some protection against the risk of litigation. Nothing in the policy could be construed as an argument for the protection of privacy as an intrinsic value. The main foundation thus appears to be consequentialist.

Turning to the question of control over data versus ownership, control is clearly to the fore. Services are available only to those who provide such information as is deemed necessary. Those who choose to register can exercise some limited control over the use of their personal data. They can opt out from its use, and also from its disclosure to third parties, for marketing purposes, but apart from this there is little further control. Personal data may be used in many ways, most of which are not described with any clarity. For example, stated uses include: 'for assessment and analysis (*e.g.*, market, customer and product analysis)' and in unspecified ways for 'the prevention and detection of fraud'. It may be passed 'to employees and agents of the Group to administer any accounts, products and services'. It may be disclosed 'to anyone to whom we may transfer our rights and duties under our agreement with you'. It may even be transferred 'to countries which do not have data protection laws or to countries where your privacy and fundamental rights may not be protected as extensively' as it is under UK legislation, and it may be combined 'with information that we receive from third parties'. Clearly, this policy is based firmly on the concept of privacy as control.

It is written almost entirely in the second person, that is, its clauses are addressed to 'you' and this is clearly meant as 'you, the customer'. The only exception is a clause that states: 'in order to protect our customers and us from fraud and theft, we may disclose...' Customers are seen as the only stakeholders with significant privacy concerns.

We know from other studies (for example, McRobb and Rogerson, 2004b) that some online privacy policies are more informative regarding the specific data collected (this policy says almost nothing) and the steps taken to protect personal data, either in transit or during storage (there is little about this, other than a vague promise to 'take all reasonable steps'). Nevertheless, Argos is not unusual in its rather defensive stance.

Unlike Argos, AT&T displays a third party trustmark (the BBB Online mark). This suggests at first glance that their privacy policy may be more informative, and that it may have more transparency. However, in its detailed content, it gives little more insight than that of Argos, despite being roughly twice the length (2821 words compared with 1537). There is no clear description of the personal data collected, except that the focus is on 'customer identifiable information'.

Customers are, however, explicitly named as such, and most of the policy is written in the third person. The AT&T policy also covers some issues not addressed by Argos, in particular the special status of young people under 18. This is probably due to the relatively high profile in the USA of the Children's Online Privacy Act.

The implied basis for privacy is chiefly, but not entirely, utilitarian. There is, however, in the opening paragraph, a reference to AT&T's 'long-standing tradition of recognising and protecting the privacy of customers', which may suggest that some intrinsic value is associated with the concept. However, the policy states that 'online services [have] created additional privacy concerns, particularly for consumers' and then goes on to explain the constraints that apply to the use and disclosure of personal information. The aim here is to reassure customers so that they will continue to engage in transactions that are profitable for the company.

For the most part, this policy frames privacy in terms of control, but one section says: 'AT&T will not sell, trade, or disclose to third parties any customer identifiable information...' While this does not quite acknowledge that privacy is an ownership issue – nor, indeed, that ownership of personal information necessarily resides with the individual described – it does at least admit that information can be seen as property.

For the most part, the policy is clearly addressed at customers, although these are sometimes called 'consumers' and sometimes addressed in the second person: 'How AT&T Protects Your Privacy Online'. One small separate section of the policy is aimed at business customers. However, its content appears to describe exactly the same privacy practices as for individual consumers. It is not clear whether this resulted from an analysis that happened to show that the two groups had identical concerns. It may indicate no more than a desire to create the impression that the interests of both groups have been separately addressed.

#### *4.4 Policies in the domain of e-government*

We chose the US Central Intelligence Agency (CIA) and the UK Inland Revenue to represent this domain. Both are large central agencies of e-government with long-established websites, although there are major differences between their online activities.

The Inland Revenue policy contains some elements that appear to suggest a consequentialist attitude, but other elements indicate more of an *a priori* attitude to privacy. It begins with a rather legalistic statement about the organisation's responsibility as 'a Data Controller under the Data Protection Act [to] hold information for the purposes of taxes, social security contributions, tax credits and certain other statutory functions...' The reference to responsibility implies an intrinsic perspective, but the statement could also be construed as defensive, and thus consequentialist in tone. A little further on, the underlying motivation is shown in a different light: 'We may get information about you from others or we may give information to them [partly in order to] protect public funds.' This is a classic utilitarian argument: your privacy may be harmed, but only in order to protect the legitimate interests of others. Still further on, we learn that the Inland Revenue has 'a legal duty to protect the confidentiality of taxpayer information'. This seems to acknowledge that privacy has an intrinsic quality, and is not simply instrumental to the achievement of some other good. This policy, then, appears to rest on a complex set of assumptions about privacy that range from the utilitarian to the intrinsic. Since the institution in question is governmental and the jurisdiction is Anglo-Saxon, this is hardly surprising.

Privacy as construed by this policy is very much a matter of control, not ownership. In this respect, it resembles the e-commerce policies. But there is a striking difference in that the Inland Revenue policy seeks to address more than one stakeholder group. It reassures those who register for a service that their data will be protected, and is reasonably clear about how it will be used and protected. This is similar to Argos. But elsewhere it implies, for example in the mention of 'statutory functions as assigned by Parliament' and other public interest concerns, that the reader may be seen as a citizen, not merely as a service consumer. The policy conveys an assumption that the reader will be pleased to learn that statutory duties are being carried out, and that the public good is being protected. This recognises that the conflict of interest in this domain is located within the individual, as we suggested in the earlier theoretical section.

The CIA policy begins with a statement that the organisation 'is committed to protecting your privacy'. Moreover, those who visit the CIA website 'do so anonymously unless you choose to provide us information about yourself'. While these statements could plausibly be underpinned by a consequentialist argument, it seems more likely that they convey an intrinsic concern for privacy. The essential characteristic of this concern for privacy is control, rather than ownership.

This policy is very clear about the nature of personal information collected, the circumstances in which it will be collected and the uses to which it will be put. This might be surprising for an organisation whose *raison d'être* is to gather secret intelligence, but the explanation may lie in the distinction between the CIA's intelligence monitoring activities (not subject to the policy) and its other, more routine administrative activities (which are subject to the policy). There is also a differentiation between different possible interests of visitors, who are not seen as one homogenous group. Several groups of stakeholders can be readily identified:

- Citizens, who are presumed to approve of the goals of the CIA
- Potential employees, who are encouraged to submit personal information, and are advised on how it will be used
- Those wishing to volunteer intelligence, who are also encouraged to submit personal information, and are advised on how it will be used

- Potential miscreants, who are warned that they will not receive the same privacy protection as other visitors
- Casual visitors, from whom no personal information will be collected.

This policy thus considers the widest range of stakeholders of any in the study.

#### 4.5 *Policies in the domain of e-teaching*

We chose Millikin University in the USA and Plymouth College of Further Education in the UK to represent this domain. Both are moderate-sized institutions in the further/higher sector, with some significant online activity for a variety of stakeholder groups.

Despite its brevity (543 words), the policy of Plymouth College of Further Education shows some complexity. Some clauses suggest a consequentialist basis for consideration of privacy. For example, some information is retained ‘to assist the College in identifying and communicating to you further products and services offered by ourselves and other commercial companies/educational establishments’. Yet, on the other hand, information is also retained ‘to monitor and comply with our Equal Opportunities and Disability Policies, and discrimination legislation’, which could perhaps be seen as consequentialist (defensive against possible litigation), but can also be interpreted as the indirect pursuit of an end for its intrinsic value. Other parts of the policy carry echoes of the Inland Revenue logic that locates the conflict of interest within the individual. For example, records are kept ‘so that we can provide references upon request’ – so your privacy may be harmed, but to serve the greater good of helping you obtain employment.

Privacy is seen as essentially a matter of control rather than ownership. But the needs of different stakeholders are considered in a very explicit manner. Stakeholder groups that can be readily identified are as follows:

- Students: ‘monitoring of your educational development’
- Customers: ‘delivery of commercial... services’
- Employees: ‘health, welfare, safety and security’
- Members of the general public: ‘use of College facilities’.

In some cases, the issues cross stakeholder group boundaries, so this identification of groups affected is tentative. But it does not appear tenable that such a range of issues could be identified without some stakeholder analysis having occurred.

Of all those considered in this study, the Millikin University policy comes closest to appearing to endorse intrinsic value arguments for privacy protection. In the first sentence, it is claimed that the University ‘respect[s] the privacy of all website visitors to the extent permitted by law’. Later statements indicate that no information will be collected unless it is volunteered, and that such information ‘will be used only for the purpose indicated’. It will not be sold, ‘exchange[d] or otherwise distribute[d]’ without consent – again, unless this is required by law. This seems to foster an image of the University’s website and online operations, such that they exist only to serve the needs of those who request services. However, since Millikin University is a private organisation that depends for its survival on success in a competitive market place, it seems likely that there is some consequentialist, profit-oriented reasoning going on in the background.

The part of the policy which concerns personally identifiable information is very brief (one paragraph of 196 words), and the online activities through which the University can gather such information appear from this document to be very limited. Moreover, only external visitors to the website are discussed, while internal stakeholders are not considered at all. However, internal stakeholders (specifically in relation to the University's online provision) certainly exist. Elsewhere on the University's website a range of services can be found that are clearly intended for students and academics. These include a secure login to a student and/or staff extranet, and an online payment facility where students can view their bills and pay their fees to the University. Some of this activity is educational, while some is essentially e-commerce in its nature. It is surprising that the privacy policy pays no attention to such potentially privacy-sensitive activities.

## **5 Conclusion**

We have argued that privacy of personal information is a key aspect of the e-phenomenon. Its importance and its characteristics vary according to the domain of the e-phenomenon, for reasons that derive partly from the nature of privacy and partly from the domain. There are various theoretical accounts of the ethics of privacy, ranging from arguments based on the Categorical Imperative to utilitarian ones. We examined how these arguments apply to practical considerations for each domain. We also highlighted the relationship between the context and the various stakeholders engaged in that context, and how this can interact with the different conceptual views of privacy. This led to some predictions about how the privacy policies of organisations might be expected to reify these conceptual considerations. Selected privacy policies from six organisations were then critically analysed from an interpretivist perspective. The results provide some insight but also raise questions that merit further investigation.

We found little sign that policymakers are interested in operationalising privacy as a form of property. It seems that privacy is seen as control, not ownership. However, the policies were mixed on the question of whether the importance of privacy rests on instrumental or on intrinsic grounds. There is some alignment with our prediction that e-government organisations are more likely to favour an intrinsic foundation for privacy, while e-business organisations are more likely to take an instrumentalist view. The e-teaching policies were more ambivalent, confirming our expectation that organisations in this domain will show some characteristics of both e-business and e-government.

The extent to which different groups of stakeholders are addressed proved interesting. The selected e-business privacy policies address only the interests of their customers, while the e-government and e-teaching organisations seem to recognise both the variety of stakeholders and the different conflicts of interest that prevail. One anomaly was the Millikin University policy, which makes no mention of students or staff despite their significant participation in its online activities.

These findings add to our understanding of the ways that privacy is interpreted in different areas of the e-phenomenon. However, the study has limitations. First, and most important, it does not address the privacy practices of the organisations, nor whether or not these relate to published policy. Second, our evidence is drawn entirely from documents that are publicly accessible on the internet. While these are certainly

primary sources, there are other sources that might give useful insight into the questions we have raised. For example, access to internal documents and sources could add considerable depth and richness to the analysis, especially regarding attitudes towards internal stakeholders.

It is also true that, while our findings provide some illumination, they cannot be generalised in any statistical sense. It may be interesting to conduct a further enquiry using methods that can lay greater claim to statistical validity. But since the primary focus of our research is on attitudes, qualitative methods are more likely to produce further illumination. For example, examination of a broader range of policies following either a grounded theory or a discourse analysis approach might produce insights that are at once more detailed and more capable of general applicability. The present study could serve as a useful precursor to such a study, chiefly by helping to demonstrate that the issues merit further examination. But this would still not meet a demand for statistically based generalisation of the results.

Despite the limitations of the paper, we hope that it has provided a useful contribution to the question of the current special issue. We believe it is not contentious to say that the e-phenomenon exists and that there are characteristics shared by different aspects of the phenomenon. Using three different industries or sectors, we have shown that privacy is a central concern to all of them. Privacy concerns have gained prominence due to the use of technology in traditional industries. At the same time, we have seen that the answers that the three sectors give to the challenges of privacy differ. This is not surprising in the light of the literature review, which pointed out that there are deep philosophical differences with regard to our understanding of privacy. What is shared by all types of organisations involved in the e-phenomenon is that they need to pay attention to the issue of privacy and that they need to give answers to the questions that we raised in this paper. Our empirical observations have shown that such answers are often implied in privacy statements but they are rarely made explicit. The main contributions of our paper will therefore be to raise awareness of the problem of privacy and the fact that there are different ways of perceiving and addressing it, and to signal the limited extent to which the problem is currently addressed in the online privacy policies that we examined.

## References

- Alavi, M. and Leidner, D.E. (2001) 'Research commentary: technology-mediated learning – a call for greater depth and breadth of research', *Information Systems Research*, Vol. 12, No. 1, pp.1–10.
- Arendt, H. (1958) *The Human Condition*, 2nd ed., Chicago: The University of Chicago Press.
- Brey, P. (2001) 'Disclosive computer ethics', in R.A. Spinello and H.T. Tavani (Eds.) *Readings in Cyberethics*, Sudbury, Massachusetts *et al.*: Jones and Bartlett, pp.51–62.
- Britz, J.J. (1999) 'Ethical guidelines for meeting the challenges of the information age', in L.J. Pourciau (Ed.) *Ethics and Electronic Information in the 21st Century*, West Lafayette, Indiana: Purdue University Press, pp.9–28.
- Brown, W.S. (2000) 'Ontological security, existential anxiety and work place privacy', *Journal of Business Ethics*, Vol. 23, pp.61–65.
- Cabinet Office (1999) *E-commerce@its.best.co.uk – A Performance and Innovation Unit Report*, [http://www.strategy.gov.uk/downloads/su/ecommm/ec\\_body.pdf](http://www.strategy.gov.uk/downloads/su/ecommm/ec_body.pdf) (accessed 5 October 2005).
- Castells, M. (1997) 'The information age: economy, society, and culture, Volume II', *The Power of Identity*, Oxford: Blackwell.

- Culnan, M.J. (1993) 'How did they get my name?: An exploratory investigation of consumer attitudes toward secondary information use', *MIS Quarterly*, Vol. 17, No. 3, pp.341–363.
- Desai, M.S., Richards, T.C. and Desai, K.J. (2003) 'E-commerce policies and customer privacy', *Information Management and Computer Security*, Vol. 11, No. 1, pp.19–27.
- Elgesem, D. (2001) 'The structure of rights in directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data', in R.A. Spinello and H.T. Tavani (Eds.) *Readings in Cyberethics*, Sudbury, Massachusetts et al.: Jones and Bartlett, pp.350–377.
- Elgesiem, D. (1996) 'Privacy, respect for persons, and risk', in C. Ess (Ed.) *Philosophical Perspectives on Computer-Mediated Communication*, Albany: State University of New York Press, pp.45–66.
- Fleming, S.T. (2003) 'Biometrics: past, present, and future', in R. Azari (Ed.) *Current Security Management and Ethical Issues of Information Technology*, Hershey et al.: IIRM Press, pp.111–132.
- Foucault, M. (1975) *Surveiller et punir: Naissance de la prison*, Paris: Gallimard.
- Gallivan, M.J. and Depledge, G. (2003) 'Trust, control and the role of interorganizational systems in electronic partnerships', *Information Systems Journal*, Vol. 13, pp.159–190.
- Gauzente, C. (2004) 'Web merchants' privacy and security statements: how reassuring are they for consumers? A two-sided approach', *Journal of Electronic Commerce Research*, Vols. 5–3, pp.181–198.
- Gavison, R. (1995) 'Privacy and limits of law', in D.G. Johnson and H. Nissenbaum (Eds.) *Computers, Ethics and Social Values*, Upper Saddle River: Prentice Hall, pp.332–351.
- Goold, B.J. (2003) 'Public area surveillance and police work: the impact of CCTV on police behaviour and autonomy', *Surveillance and Society*, Vol. 1, No. 2, pp.191–203.
- Greenaway, K.E. and Chan, Y.E. (2005) 'Theoretical explanations for firms' information privacy behaviors', *Journal of the Association for Information Systems*, Vol. 6, No. 6, pp.171–198.
- Himanen, P. (2001) *The Hacker Ethic and the Spirit of the Information Age*, London: Secker and Warburg.
- Huynh, M.Q., Umesh, U.M. and Valacich, J.S. (2003) 'E-learning as an emerging entrepreneurial enterprise in universities and firms', *Communications of the Association for Information Systems*, Vol. 12, pp.48–68.
- Introna, L. (2000) 'Privacy and the computer – why we need privacy in the information society', in R.M. Baird, R. Ramsower and S.E. Rosenbaum (Eds.) *Cyberethics – Social and Moral Issues in the Computer Age*, New York: Prometheus Books, pp.188–199.
- Introna, L. (2003) 'Workplace surveillance "is" unethical and unfair', *Surveillance and Society*, Vol. 1, No. 2, pp.210–216.
- Johnson, D.G. (2001) *Computer Ethics*, 3rd ed., Upper Saddle River, NJ: Prentice Hall.
- Johnson-Page, G.F. and Thatcher, R.S. (2001) 'B2C data privacy policies: current trends', *Management Decision*, Vol. 39, No. 4, pp.262–271.
- Klein, H.K. and Huynh, M.Q. (2004) 'The critical social theory of Jürgen Habermas and its implications for IS research', in J. Mingers and L. Willcocks (Eds.) *Social Theory and Philosophy for Information Systems*, Chichester: Wiley, pp.157–237.
- Leidner, D.E. and Jarvenpaa, S.L. (1995) 'The use of information technology to enhance management school education: a theoretical view', *MIS Quarterly*, Vol. 19, No. 3, pp.265–291.
- Mason, R.O. (1986) 'Four ethical issues of the information age', *MIS Quarterly*, Vol. 10, pp.5–12.
- McRobb, S. and Rogerson, S. (2004a) 'Are they really listening? An investigation into published online privacy policies', *Information Technology and People*, Vol. 17, No. 4, pp.442–457.
- McRobb, S. and Rogerson, S. (2004b) 'Privacy policies online: reflections on a continuing investigation', *Proc EthiComp*, Syros, Greece.

- McRobb, S. and Rogerson, S. (2005) 'Privacy policies online: further reflections from a continuing investigation', *Proc EthiComp*, Linköping, Sweden.
- Milne, G.R. and Culnan, M.J. (2002) 'Using the content of online privacy notices to inform public policy: a longitudinal analysis of the 1998–2001 US web surveys', *The Information Society*, Vol. 18, pp.345–359.
- Moor, J.H. (2000) 'Toward a theory of privacy in the information age', in R.M. Baird, R. Ramsower and S.E. Rosenbaum (Eds.) *Cyberethics – Social and Moral Issues in the Computer Age*, New York: Prometheus Books, pp.200–212.
- Nissenbaum, H. (2001) 'Toward an approach to privacy in public: challenges of information technology', in R.A. Spinello and H.T. Tavani (Eds.) *Readings in Cyberethics*, Sudbury, Massachusetts *et al.*: Jones and Bartlett, pp.392–403.
- Nye, D. (2002) 'The "privacy in employment" critique: a consideration of some of the arguments for "ethical" HRM professional practice', *Business Ethics: A European Review*, Vol. 11, No. 3, pp.224–232.
- Piccoli, G., Ahmad, R. and Ives, B. (2001) 'Web-based virtual learning environments: a research framework and a preliminary assessment of effectiveness in basic IT skills training', *MIS Quarterly*, Vol. 25, No. 4, pp.401–426.
- Robison, W.L. (2000) 'Privacy and appropriation of identity', in G. Collste (Ed.) *Ethics in the Age of Information Technology*, Linköping: Centre for Applied Ethics, pp.70–86.
- Rogerson, S. (1998) *Ethical Aspects of Information Technology – Issues for Senior Executives*, London: Institute of Business Ethics.
- Rotenberg, M. (1998) 'Communications privacy: implications for network design', in R.N. Stichler and R. Hauptman (Eds.) *Ethics, Information and Technology: Readings*, Jefferson, NC: MacFarland and Company, pp.152–168.
- Severson, R.J. (1997) *The Principles of Information Ethics*, Armonk, New York/London: M.E. Sharpe.
- Sipior, J.C. and Ward, B.T. (1995) 'The ethical and legal quandary of email privacy', *Communications of the ACM*, Vol. 38, No. 12, pp.48–54.
- Spinello, R. (2000) *Cyberethics: Morality and Law in Cyberspace*, London: Jones and Bartlett.
- Stahl, B.C. (2004) 'Responsibility for information assurance and privacy: a problem of individual ethics?', in C.D. Schou and K.J. Trimmer (Eds.) *Journal of Organizational and End User Computing*, Special Issue on Information Assurance and Security, Vol. 16, No. 3, pp.59–77.
- Stahl, B.C. (2005) 'The paradigm of e-commerce in e-government and e-democracy', in W. Huang, K. Siau and K.K. Wei (Eds.) *Electronic Government Strategies and Implementation*, Hershey PA: Idea Group Publishing, pp.1–19.
- Stahl, B.C., Prior, M., Wilford, S. and Collins, D. (2005) 'Electronic monitoring in the workplace: if people don't care, then what is the relevance?', in J. Weckert (Ed.) *Electronic Monitoring in the Workplace: Controversies and Solutions*, Hershey, PA: Idea-Group Publishing, pp.50–78.
- Stalder, F. (2002) 'Privacy is not the antidote to surveillance', *Surveillance and Society*, Vol. 1, No. 1, pp.120–124.
- Straub, D.W. and Collins, R.W. (1990) 'Key information liability issues facing managers: software piracy, proprietary databases, and individual rights to privacy', *MIS Quarterly*, Vol. 14, pp.143–156.
- Tavani, H. (2000) 'Privacy and security', in D. Langford (Ed.) *Internet Ethics*, London: McMillan, pp.65–89.
- Tavani, H.T. and Moor, J.T. (2001) 'Privacy protection, control of information, and privacy-enhancing technologies', in R.A. Spinello and H.T. Tavani (Eds.) *Readings in Cyberethics*, Sudbury, Massachusetts *et al.*: Jones and Bartlett, pp.378–391.
- Tress, M. (2000) 'e-Learning accelerates and transforms business school pedagogy', *A Special Report to AACSB Annual Meeting*, San Diego, CA: SmartForce, 9 April.

- Urbaczewski, A. and Jessup, L.M. (2002) 'Does electronic monitoring of employee internet usage work?', *Communications of the ACM*, Vol. 45, No. 1, pp.80–83.
- van den Hoeven, J. (2001) 'Privacy and the varieties of informational wrongdoing', in R.A. Spinello and H.T. Tavani (Eds.) *Readings in Cyberethics*, Sudbury, Massachusetts *et al.*: Jones and Bartlett, pp.430–442.
- van den Hoven, J. (1999) 'Privacy or informational injustice?', in L.J. Pourciau (Ed.) *Ethics and Electronic Information in the 21st Century*, West Lafayette, Indiana: Purdue University Press, pp.139–150.
- Velasquez, M. (1998) *Business Ethics: Concepts and Cases*, 4th ed., Upper Saddle River, NJ: Prentice Hall.
- Warren, S.D. and Brandeis, L.D. (1890) 'The right to privacy', *Harvard Law Review*, Vol. 5, pp.193–220.
- Weckert, J. and Adeney, D. (1997) *Computer and Information Ethics*, Westport, Connecticut/London: Greenwood Press.
- Weisband, S.P. and Reinig, B.A. (1995) 'Managing user perceptions of email privacy', *Communications of the ACM*, Vol. 38, No. 12, pp.40–47.
- Yoon, S-H. (1996) 'Power online: a post-structuralist perspective on computer-mediated communication', in C. Ess (Ed.) *Philosophical Perspectives on Computer-Mediated Communication*, Albany: State University of New York Press, pp.171–196.

## **Bibliography**

- Argos Limited (2004) *Privacy Policy*, <http://www.argos.co.uk/static/StaticDisplay/includeName/privacyPolicy.jsp.htm> (accessed 6 July 2005).
- AT&T (2005) *Privacy Policy*, [www.att.com/privacy/](http://www.att.com/privacy/) (accessed 6 July 2005).
- Central Intelligence Agency (2005) *Privacy Notice*, [www.cia.gov/cia/notices.html#priv](http://www.cia.gov/cia/notices.html#priv) (accessed 5 July 2005).
- Inland Revenue (2005) *Privacy Policy*, <http://www.hmrc.gov.uk/about/privacy.htm> (accessed 10 December 2004).
- Millikin University (2005) *Online Privacy Statement*, <http://www.millikin.edu/privacy.asp> (accessed 18 October 2005).
- Plymouth College of Further Education (2005) *Privacy Statement*, <http://www.pcfce.ac.uk/privacy.html> (accessed 5 October 2005).
- Wikipedia (2006) *Definition of Electronic Commerce*, <http://en.wikipedia.org/wiki/E-commerce> (accessed 17 March 2006).