ICIS 2005 Proceedings

International Conference on Information Systems (ICIS)

December 2005

Privacy Implications of Technology Innovation Processes

Karl Prince
University of Cambridge

Michael Barrett
University of Cambridge

PRIVACY IMPLICATIONS OF TECHNOLOGY INNOVATION PROCESSES

Karl Prince and Michael Barrett
Judge Business School
University of Cambridge
Cambridge, United Kingdom
kjp30@cam.ac.uk **m.barrett@jbs.cam.ac.uk**

Abstract

The focus of this study is on furthering our understanding of the relationship between technology and privacy by examining privacy concerns during the innovation process. We begin by exploring the techno-privacy relationship and what it is about technology that so concerns us. Dealing with privacy concerns of already developed and adopted technologies is difficult, and we propose that a focus early on as to how stakeholders deal with privacy concerns during the innovation process could be an effective strategy. We start our investigation by drawing on the work of Introna and Pouloudi (1999), whose principles of representation, access, and power aid the analysis of privacy concerns in the information age. We present a qualitative research case study that followed the efforts of three particular stakeholder groups in dealing with privacy concerns raised during a technology innovation process. The analysis provides empirical evidence for Introna and Pouloudi's principles. We develop two further interrelated concepts, organizational image and timing, which our analysis suggests are specific to understanding how stakeholders deal with privacy during the innovation process.

Keywords: Technology innovation, privacy

Introduction

While technologies may be designed and initially developed for particular purposes, they often affect society in ways not imagined originally. A specific example of this is the interaction between technology and privacy. Often new information technologies are developed with what seem initially as benign designs and yet later are considered to have capabilities that threaten the privacy of individuals. The relationship between technology and society has been a focus for much research aimed at understanding how technology is developed and in turn shapes society (Lyon 1994).

Current literature related to technology and privacy includes a focus on identifying consumer issues related to the use of new technology such as the Internet. These include studies of online consumer privacy (Hine and Eve 1998), studies with particular focus on issues such as the viability of self-regulation (Culnan 2000) or finding a balance in the trade-off between consumer benefits and privacy (Culnan and Bies 2003). Research aimed at understanding privacy in the information age is centered on information privacy (Culnan and Armstrong 1999; Kang 1998). Other work has focused on understanding the privacy of users within technology environments or in using technology. Examples of this include Webster's (1998) work on desktop video-conferencing and privacy concerns and Bellotti and Sellen's (1993) work on computer-supported collaborative work in ubiquitous computing environments that has been further developed to include the concept of ubiquitous computing environments (Lederer et al. 2002). One of the general concerns is whether the accelerated pace of technological developments will continue to erode the levels of privacy we have today. Once technologies have been developed and have become embedded in society, it is difficult to raise privacy concerns resulting from the use of the technology, whether because of fear of sanction, a sense of fatalism, or simply a lack of awareness (Marx 2003b). It is also a nontrivial task to remove or change the technology to accommodate, amongst other concerns, privacy claims (Marx 2003a). The most common strategies for protecting privacy are the use of various

Table 1. Principles Aiding Analysis of Privacy Issues (Introna and Pouloudi 1999)

Representation Who is present during negotiations of privacy claims?
Access What information is made accessible to those represented?
Power How do relationships of power affect the negotiation of privacy claims?

forms of legislation, such as the European Union's Data Protection Directive, self-regulation, such as an industry code of conduct, and privacy enhancing technologies (PETs), such as data encryption. Yet many of these solutions for dealing with privacy center on post technology development treatments (e.g., legislation lags behind technological development and PETs generally attempt to solve problems raised by technologies after development is completed). This is not to say that they do not play an important role in protecting privacy but it may be constructive to consider ways to deal with privacy concerns during development in the innovation process, rather than the more common and problematic attempts at dealing with concerns after development and adoption.

Focusing on the innovation process is important as it is during these early stages that privacy concerns may already become evident. As a starting point we use three principles proposed by Introna and Pouloudi (1999) to aid the analysis of privacy claims and risks. These principles, listed in Table 1, were proposed to present "an analytic ability to proactively identify and understand privacy/transparency risks" (Introna and Pouloudi 1999, p. 36).

In the next section, we discuss the relationship between technology and privacy. We go on to detail the principles proposed by Introna and Pouloudi for analyzing issues of privacy. We then present a case study that explores more specifically how various stakeholders deal with issues of privacy during the innovation process based on the development of a ubiquitous technology. Through our analysis of the empirical data, we identify further factors related to privacy that are particular to the innovation process. By identifying privacy concerns as early as possible and understanding how the various actors deal with them it may be possible to develop technological innovations in a way that proactively mitigates privacy risks and enhances their potential for successful adoption.

Technology and Privacy

The relationship between technology and privacy is not new. From the earliest defenses of a right to privacy threatened by technological progress (Warren and Brandeis, 1890) through the expansive use of automated data processing technologies in the 1960s and 1970s (Westin 1967) to the modern day rise of the Internet, technology has influenced the concept of privacy. Despite much research and debate about privacy, however, attempts at reaching consensus on what a suitable definition for privacy might be have not met with much success (Gellman 1998; Parent 1983; Schoeman 1984). Privacy has been described as the right to be left alone (Warren and Brandeis, 1890), the control over the intimacies of personal identity (Gerety 1977), the control of information about oneself (Westin 1967), the control of access to oneself (Altman 1975, 1977) and the limitation of access to oneself (Gavison 1980).

One particular definition of privacy that has been suggested by Introna and Pouloudi (1999) as being suitable for investigating privacy issues in the information society is Johnson's (1989) judgement-of-others model. Johnson proposes that the many examples of privacy have one thing in common: "they are aspects of a person's life which are culturally recognized as being immune from the judgement of others" (p. 157). This freedom from judgement of others, however, is not absolute and there is no general immunity from judgement but there are certain aspects of a person's life that should be shielded from the evaluative judgements of others, knowing that one may be judged according to the norms, values, and unsuitable ideas of others (Introna and Pouloudi 1999). Acknowledging this need to maintain a level of privacy in life, Johnson includes the concept of control, typically regarded as central to the concept of privacy, in his privacy model (i.e., individuals have the right to control who forms evaluative judgements about themselves), the aim being to limit, not eliminate, judgement. Johnson extends his privacy model to include not only the conscious judgements of others but also the "unwarranted emotional attitudes of others" (p. 166). An individual, therefore, is not only concerned when someone else judges them according to their personal information but also by the emotional involvement of the other person in their lives, especially if the emotion is expressed strongly. We use the judgement-of-others privacy model to illuminate the ways in which technology affects privacy by taking a closer look at some specific characteristics of technology.

Technological Characteristics and the Judgement of Others

One of the more obvious characteristics of technology is the facility to collect large volumes of data. Records are kept on every aspect of an individual's life and few can survive as members of society without providing the necessary information for these records. Related to this are the capabilities technologies provide to search through volumes of data and to aggregate data from various sources. This enables seemingly insignificant pieces of information to be located and linked, creating more detailed sets of information. According to the judgement-of-others models, the concern is that individuals have little control over who has access to their personal data and the judgements formed based on this data. Technology makes it easier to capture and store information related to what may seem transient events or states, resulting in more permanent records. This persistence of information may affect an individual's perception of what is really private, for example, enabling a seemingly innocuous statement made by a celebrity today to be recorded and used at a much later date to make judgements on their character. This further increases the information data set which others may use to form judgements about an individual and limits the domain of information that may be regarded as private. Technology often makes the data gathering process seem invisible to an individual: one cannot tell that data is being gathered and, even if you know of the capability, the fact that it happens unobtrusively means that you are not alerted to it. Even if one has given consent for data to be collected for an original purpose, the potential future uses of the data may change. As individuals may be unaware that their data is accessed, they have little control over how their information is interpreted or any inappropriate judgements made based on norms and values in conflict with the original intention of the data capture.

A further characteristic of rapidly developing technologies is that of ubiquity or pervasiveness. Increasingly ubiquitous technologies provide more opportunities to gather private information resulting in more ways that others may potentially form judgments of one another. At the same time, the pervasiveness of technology aimed at collecting more and more data can be interpreted as an increase in the intensity of the interest in the lives of others (e.g., companies want to know increasingly more about their customers). As discussed earlier, this increasing interest in people's lives implies emotional involvement and that in itself is an undesirable judgement, for example, we are not only concerned by whatever conscious judgements may be made but also by the emotional involvement of others in our lives, even more so when that emotion is expressed intensely (Johnson 1989). Furthermore, all of these technological characteristics together also have the potential to affect privacy and combined could potentially hold a greater risk to privacy. As Introna and Pouloudi describe it, the differences between ones own values and interests and those of others are compounded by technological capabilities that may enable completely unsuitable ways in which one may be judged.

Technology Innovation and Privacy

We have previously argued that it may be beneficial to attempt to deal with privacy concerns as early as possible, before development is completed (i.e., during the technology innovation process). In trying to deal with privacy concerns raised during the innovation process, it may be possible to alter the technology itself to try and maintain acceptable levels of privacy or avoid potential future violations when the technology is ultimately adopted. As a first step to developing strategies for dealing with privacy issues during technology innovation, we focus on developing an understanding of how different stakeholders deal with privacy concerns during the innovation process. This will enable us to consider ways in which it may be possible for technologies to be developed having given due consideration to privacy concerns. We draw on the work of Introna and Pouloudi as an initial basis for investigating how issues of privacy are dealt with by various stakeholders, a term which we clarify in the next section. Introna and Pouloudi propose three principles to aid in the analysis of potential issues of privacy in order to "identify and make explicit privacy…risks" (p. 33): the principles of representation, access, and power. These principles not only ensure that privacy concerns of all stakeholders are made explicit and taken into account but could also be used for evaluating systems and procedures aimed at maintaining privacy.

The *representation* principle requires that all stakeholders be present when privacy claims are considered. Stakeholders may either be physically present or may be represented by another stakeholder. What is important is that all stakeholders should be able to participate in some way when negotiating privacy claims. The *access* principle requires that only information relevant to the particular context of the privacy claims being judged be made available to stakeholders. This is necessary since it is not possible for stakeholders to "separate information, values and interests in making judgements about others" (Introna and Pouloudi 1999, p. 33). If irrelevant information is introduced while privacy claims are being negotiated it would not be possible for stakeholders to simply ignore such information, instead it is likely that their decisions will be affected by all the information presented, relevant or irrelevant. One of the concerns, however, is who decides what information is relevant or irrelevant. This question is affected by the last principle, that of power. The *power* principle relates to the notion that stakeholders enter into privacy claims not only with their own interests and values but also with existing relationships of power and influence. Ideally all stakeholders in a privacy claim would be equal, having the same access to information and an equal ability to represent their interests and values. Unfortunately this is not always practically feasible and individual or groups of stakeholders may be able to manipulate privacy claims in their own favor by, for example, keeping information to themselves or ensuring that another stakeholder is not represented. If stakeholders are unable to take into account and manage the principles of representation, access, and power when dealing with privacy concerns, it could result in claims being unacknowledged or under represented and the ultimate violation of a stakeholder's privacy through inappropriate judgements.

One criticism of the principles proposed by Introna and Pouloudi is that it enables an analysis of how actors deal with privacy issues in broader, generalized settings (i.e., they are relevant at almost any stage of the technology life-cycle, from the earliest innovation steps through implementation and adoption). We argue that there are other conceptual elements specific to the innovation process that may additionally affect how issues of privacy are managed by the various stakeholders. There has also been limited application of the principles to empirical data and as such the applicability of the principles remains untested. In the following empirical research, we aim to investigate not only the relevance of these general principles but also the significance of any specific concepts related to the innovation process.

An Empirical Investigation

The empirical study presented here was conducted as part of a broader research project of a technology innovation process. During the technology development process, the issue of privacy became prominent and presented an opportunity to investigate more closely the relationship between privacy and technology. The research conducted was based on a qualitative research methodology. The primary source for data was 30 semi-structured interviews with individuals—including research directors, CEOs, and technology program directors—within identified stakeholder groups in the context of the technological innovation. Secondary data sources such as meeting notes and news articles were also used to support the primary data sources. The qualitative data was initially coded as part of the analysis of a larger research project. After privacy concerns had been identified as a significant theme, the data was categorized using the broader principles of the Introna and Pouloudi (1999) framework discussed earlier. Further categorizations were analyzed for their relevance to privacy issues and technology innovation in an effort to explore relevant themes beyond these general principles.

The Case Study: ConnectNet

In October 1999, the ConnectNet Centre was founded by a group consisting of a renowned university, two global standards bodies, and two global, fast-moving consumer goods companies. The ConnectNet Centre's focus was the development of a technology described as "the Internet of things"—the PhysNet. PhysNet was envisioned by the Centre as a ubiquitous technology capable of identifying billions of products uniquely in an interconnected network that included everyday physical objects. The innovation is based on radio frequency identification (RFID) technology. Similar to a bar code, an RFID tag, consisting of an integrated circuit chip and an antenna, is placed on an object in order to uniquely identify it and facilitate tracking of the object. Unlike a bar code, an RFID tag does not need to by scanned physically but can be read automatically by readers. Furthermore, by creating a network connection, the tag could be linked to databases containing further detailed product information. In this way, ordinary objects, not only computers, could become part of the broader network we call the Internet today.

In this study the issue of privacy in the PhysNet innovation process is investigated using the perspectives of various stakeholder groups. The stakeholder concept in the broader management literature as well as more specifically in information systems has been defined in a number of ways. Using Freeman's (1984) definition of stakeholders as a basis, Pouloudi and Whitley (1997), in their study of interorganizational information systems, consider stakeholders to be "particular individuals, groups and organizations who can affect or be affected by the inter-organizational system" (p. 1). Furthermore, they distinguish between two groups in systems development: *participants*, the individuals, groups and organizations who take part in the development process, and *stakeholders*, the aforementioned participants as well as "other individuals, groups or organizations whose actions can influence or be influenced by the development and use of the system whether directly or indirectly" (p. 2). Although such a definition might be considered very broad, the advantage is that it allows the researcher to consider a wide range of potential stakeholders that may otherwise have been ignored. The definition is also relevant for a technology that is not only developed in an interorganizational network but whose intended use is as an interorganizational tool. The stakeholder groups used in this study are the ConnectNet Centre, sponsor companies, and privacy advocates (see Table 2). While the Centre and sponsor companies were participants in the development process, privacy advocates were influenced by the PhysNet development and also aimed to influence this development. These stakeholder groups were the most vocal and visible in raising and dealing with privacy concerns. Other stakeholder groups, such as government, were investigated for their relevance but were found to have less impact during the case study investigation.

Table 2. Stakeholder Groups Identified in ConnectNet Case Study

ConnectNet Centre • Six university-based research centers around the world. • Management, administration, and research staff. • Independent: working together *with* industry rather than only *for* it.
Sponsor Companies • Sponsor companies joined the ConnectNet Centre as paying members gaining early access to research and the opportunity to influence the innovation process. • Two groups: end users and technology vendors—approximately 100 companies. • End users: mainly from retail sector including some of the world's largest retailers and retail manufacturers. • Technology vendors: smaller entrepreneurial firms as well as larger global technology providers.
Privacy Advocates • Predominantly based in the United States. • Small to very small organizations. • Aimed to represent consumer interests in a mainly industrial based initiative. • Most operated independently. Few worked directly with ConnectNet Centre.

After a few years of initial development, the PhysNet technology had become more widely known. As part of the increasing interest in the technology, questions were being raised as to the potential privacy violations the technology may hold. Most of these privacy concerns were raised by privacy advocates whose arguments centered on consumer privacy. The main privacy concern stated by privacy advocates was that because PhysNet would be capable of identifying, tracking, and tracing individual products it would be possible to identify, track, and trace people associated with those products. This concern can be analyzed by highlighting the technological capabilities of PhysNet as discussed earlier. Being able to identify individual items means an increase in the *volume* of data being collected, with the potential to collect more and more specific information about an individual. The potential to trace individuals means that the simple transient act of walking through a doorway can possibly be recorded for more *permanent* record keeping. Since the technology is wireless, such tasks could be accomplished *unobtrusively*, leaving consumers unsure as to when they are being observed. *Ubiquity* was a key characteristic of the original ConnectNet Centre vision for the technology that means there is the potential for information to be gathered almost anywhere at almost anytime.

Case Analysis

The following analysis is focused on understanding how the different stakeholders attempted to deal with privacy concerns during the innovation processes of the PhysNet development.

Themes of Representation, Access and Power

The leadership of the ConnectNet Centre recognized relatively early on in the innovation process the potential privacy concerns associated with the PhysNet technology. Their own research, based on expert witnesses and a focus group study, indicated that consumers would be alarmed at the development of the technology despite the potential benefits. But the Centre and sponsor companies were selective as to which privacy advocates were represented in the privacy research conducted. In particular, they sought to work with a few advocates who they regarded as being reputable rather than those who were perceived as belonging to the more vocal groups that were beginning to create some "noise" regarding PhysNet.

> There's a lot of advocacy groups around….We've worked with what we believe are the ones with the most respect and…credibility. [ConnectNet Centre Manager]

But these interactions were limited, as one ConnectNet Centre researcher put it:

> So basically my point here is that they didn't invite all the stakeholders. They just brought these end users and the technology vendors and they brought the academics, full stop.…They failed to bring all the stakeholders on board.

It could be argued that one of the consequences of a limited representation of privacy advocates, and thereby not acknowledging this stakeholder group's claims, was the increase and intensity of resistance that followed. Privacy advocates became more outspoken, calling for the innovation process to be halted while more detailed studies of the privacy claims were conducted.

> We are requesting manufacturers and retailers to agree to a voluntary moratorium on the item-level RFID tagging of consumer items until a formal technology assessment process involving all stakeholders can take place.…Some uses of RFID technology are inappropriate in a free society, and should be flatly prohibited. Society should not wait for a crisis involving RFID before exerting oversight. [RFID Position Statement of Consumer Privacy and Civil Liberties Organizations]

Privacy advocates regarded themselves as representatives of consumer interests and values and, therefore, they considered it important that they be involved in the PhysNet privacy debate. Their role was to voice the privacy concerns of the technology that would have significant impact on the privacy of consumers in the future. They felt that consumers had limited access to information and were too removed from the innovation process to be able to have significant influence in voicing their concern. Privacy advocates could do this by representing consumers in privacy claims and ensuring that their concerns were acknowledged. Since consumers had limited access to information, privacy advocates attempted to pass what they deemed as relevant information on to the broader public. Much of this was done through traditional media such as the press but also through new media such as the Internet. Privacy advocates' websites played an important part in ensuring that information regarding the PhysNet technology was made available to anyone who needed it to make an informed decision regarding the technology.

> The Internet is an extremely effective way of communicating with people all over the place and getting your message across. [Privacy Advocate]

> When I…posted something about [a PhysNet trial] on our website, members contacted members who contacted other people…I mean it was just like an explosion of information throughout the Internet and people were calling [the sponsor company] in droves. [Privacy advocate]

But the ConnectNet Centre and sponsor companies questioned the type of information made available by the privacy advocates. They felt that advocates had a limited understanding of the technology and were not necessarily qualified to provide access to correct information. On the other hand advocates were distrustful of the ability for the Centre and industry to provide access to information that enabled others to form an adequate judgement of the technology.

It was important for the Centre and sponsor companies to ensure that they had access to information to further the development of the technology leading to its adoption. Information regarding privacy issues was disseminated in some of the regular meetings held by the ConnectNet Centre. Much of the ConnectNet Centre's work on privacy issues could be interpreted as being directed internally at the sponsor companies with the aim of convincing them that the privacy issues being raised were legitimate and needed to be addressed. Advocates felt that this internal focus meant they had limited access to information that would allow them to participate fully in the privacy debate. Such was their concern that they were not being granted access to the information and that the Centre and sponsor companies were hiding information that they breached the Centre's website, gaining access to confidential documents that showed how the ConnectNet Centre intended dealing with potential privacy concerns and the advocates themselves. The information accessed in this manner contributed to the privacy claims of privacy advocates that the ConnectNet Centre and sponsor companies could not be trusted with confidential consumer information as they could not protect their own, and furthermore they were prepared to conceal information and attempt to quieten privacy advocates rather than deal credibly with privacy concerns.

> So basically it was a very bad advertisement and affected the image for the [ConnectNet] Centre because they say…they are going to look after our privacy and they cannot look after their own privacy. That was the message [after privacy advocates] got all these…confidential documents. [ConnectNet Centre Researcher]

It was evident that privacy claims could not be made equally by the different stakeholders. Powerful global companies with access to considerable resources were sponsors of the ConnectNet Centre. Similarly, the research centers were affiliated with well-known universities across the world with recognized research capabilities of their institutions and staff.

> In my experience I found it to have helped [the technology development] because they're such strong companies and that they have a reputation for making things happen. [ConnectNet Centre Manager]

> [The] role [of the Centre staff] was particularly important because they could speak from a real base of knowledge and understanding and certainly a point of respect in terms of talking to other people. [Senior manager of a sponsor company]

The imbalance of power was evident in the ability of the ConnectNet Centre and sponsor companies to choose with whom to work (i.e., selected privacy experts and not those advocates they considered irrelevant). Furthermore, privacy advocates were typically smaller organizations with access to limited resources. With a limited capability to represent their privacy concerns, these groups had to be selective in choosing the issues on which they dedicated their resources. This lack of power was particularly noticeable where limited human resources meant that privacy advocates found it difficult to ensure their concerns were represented and acknowledged.

> There were concerns of protest and you looked outside [of the industry symposium] there were half a dozen people. I mean it's just, one or two people. [CEO of a sponsor company]

Themes Relating the Innovation Process and Privacy

Among the ConnectNet Centre and sponsor companies, many held the opinion that the Centre and technology companies were competent and knowledgeable about the technology; after all they were the ones who were developing it. Similarly the view held of those sponsors who would be adopting the technology was that they had a powerful influence on the future of the technology (i.e., should they adopt the technology, there was a good chance that wider adoption would be a success). The Centre and many of the sponsor companies believed that collectively they had a thorough understanding of PhysNet's potential and its limitations and, therefore, were capable of representing valid privacy claims associated with the innovation. The view the ConnectNet Centre and sponsor companies held of privacy advocates influenced whether they thought advocates should be allowed to represent their privacy concerns. Privacy advocates were described by the Centre and sponsors as not understanding the technology and its limitations. They had made outrageous claims on the potential privacy violations that PhysNet could enable. The Centre and sponsor companies noted that historically there were always those who complained about new technologies and resisted change but most often the technologies proved to be beneficial for society.

> Reading some of what I've read about what's been published by the advocates for getting rid of [PhysNet]… it doesn't seem to be that they really understand totally the limitations of the technology. [Senior manager of a sponsor company]

Many of the privacy advocates were aware of this view and how it may have affected their ability to make privacy claims and allow them to participate as stakeholders in resolving privacy issues. They did, however, find it difficult to change this perception.

> There's been actually some rather negative portrayals of the privacy advocates in the media…it almost seemed like there was an effort afoot…to discredit what we were saying. And also to discredit us in terms of our knowledge of the RFID technology, saying that we didn't understand the technology, the concerns that we have are overblown because the technology doesn't even allow things to happen the way we see it. [Privacy advocate]

On the other hand a ConnectNet Centre advisory group acknowledged that privacy advocates had a role to play in highlighting potential future privacy impacts. But they cautioned that there was a limit to this role and overstepping this limit by creating illegitimate privacy claims created the image of privacy advocates as Luddites. Significantly, even if only a small group of privacy advocates were responsible for making illegitimate claims, the other stakeholders would regard all advocates in the same light. This meant that often the ConnectNet Centre and sponsor companies thought that many of the advocates' privacy claims were of little significance. The image privacy advocates held of sponsor companies was of companies who, with considerable power and influence, were part of an industry that had developed technologies in the past which had significant privacy implications. For privacy advocates, therefore, it was imperative that the interests and views of sponsor companies during privacy claims be balanced with the interests and views of other stakeholders.

> Every technology that comes in always promises to bring in a better world and always promises to usher in a better society. And history shows us that that's not always the case.…You need someone to say, "Look this could happen, this is the potential." They're not going to come up with it on their own. [Privacy advocate]

Privacy advocates saw the ConnectNet Centre as an organization that did much of its work in secrecy and was unwilling to allow other stakeholders whom they deemed as irrelevant access to their operations that related to privacy concerns. Privacy advocates felt that the Centre did not have the interests of consumers at heart and if unchecked would develop PhysNet in ways that would threaten consumer privacy.

> It seems clear that part of their whole [public relations] strategy was to really not be a part of the whole public game but rather to advise…behind the scenes. [Privacy advocate]

Although the ConnectNet Centre recognized relatively early during the innovation process that privacy would be a concern, it was not completely effective in dealing with privacy claims.

> I think the ConnectNet Centre early on mentioned the privacy discussion but probably we didn't expect [the actions of a particular privacy group]. We could have done way more, although we did a lot but we could have done way more to talk about that issue. [ConnectNet Centre researcher]

Much of this ineffectiveness was due to the time required in getting sponsor companies to recognize the urgency of having to deal with privacy claims. It also proved difficult to get the various sponsor companies to reach consensus on how to deal with the privacy claims. Agreed upon privacy guidelines were only reached in the final stages of the Centre's operations.

> [When the] Centre tried to adopt principles on privacy [it found out] that different parties want to approach it differently. And so it's been perhaps more difficult than people thought to arrive at a consensus position on how to deal with the issue. [Senior manager of a sponsor company]

Sponsor companies may have had another incentive to try and control when privacy claims were engaged. Privacy claims could be regarded as a constraint on the PhysNet innovation, limiting the potential capabilities that the technology may be able to reach, in turn limiting the potential economic gain to be made. This "wait and see" approach would give companies time to determine the feasibility of the developing technology.

> I think the leadership of the center underestimated the potential resistance for corporate entities to act proactively in areas like privacy…it's my observation that corporate institutions want to kind of maximize their possibilities and not cut off opportunities before they understand what the potential future is. And the privacy issues were basically cutting off opportunities, they see this as foregoing particular kinds of things that we might do. [ConnectNet Centre policy committee member]

Privacy advocates also point to the importance of timing. They recognize that once technologies become entrenched it is difficult to deal with privacy claims. Therefore it as important that they are allowed to represent their interests and values and are given access to the innovation process as early as is necessary in order to reach appropriate judgements of privacy claims.

> They should have just been up-front from the very beginning and invited [the privacy groups] to discuss RFID with them.…their discussions showed that they were not being at all up-front and [they] thought that they could manipulate the privacy, manipulate the whole issue. [Privacy advocate]

Case Discussion

In the analysis of how stakeholders dealt with privacy concerns during the development of PhysNet, we have applied Introna and Pouloudi's principles of representation, access, and power (see Table 3). As suggested earlier, these principles are a general set, applicable to broad range of technology settings and at different stages of the technology life cycle.

Representation: The major privacy concern of the PhysNet technology was centered on the potential impact the technology held for consumers who were not directly represented during the privacy debate. Instead, privacy groups aimed to represent the interests and values of consumers although the representation of privacy groups was not uniform. Those groups regarded as fringe were not well represented within the network of research centers and sponsor companies. This limited representation meant that there was a marked difference in the understanding of what the privacy concerns were between some stakeholders (i.e., the privacy concerns of some stakeholders were not shared by the ConnectNet Centre and sponsor companies). Different stakeholders can have different perspectives of what the privacy concerns actually are, which makes identifying and dealing with privacy risks more difficult.

Table 3. General Principles for Analyzing Privacy Concerns During the Innovation Process
Representation • A stakeholder can represent not only their own interests and values but also those of others. • Limited stakeholder representation can result in different interpretations of privacy concerns.
Access • A stakeholder can limit or enhance another's access to information. • A stakeholder can forcefully gain access to information.
Power • Stakeholders have varying abilities to represent privacy concerns. • A stakeholder can attempt to control the flow of information (e.g., what information is available to other stakeholders).

Access: Throughout the PhysNet privacy debate, access to information was important. Stakeholders can attempt to enhance access to information, such as privacy advocates and the ConnectNet Centre making information available for the media and broader public. The access is important to enable the stakeholders such as consumers to be able to make judgements regarding a new technology, but one concern for stakeholders is the information that is being made accessible (i.e., is the information correct and can others form adequate judgements regarding the technology based on the information to which they have access). Importantly, not all stakeholders may have access to the same information. Even if this is done unintentionally, those stakeholders with limited access may question the motives of why access is being withheld, leading to attempts to gain access. In the ConnectNet case, the limited access to some information was interpreted by privacy advocates as a cause for concern, a deliberate attempt to limit the representation of other stakeholders, and brought into question the motives of the Centre and sponsor companies.

Power: The power principle affects both the representation and access principles. Stakeholders have the ability to ensure that their own interests and values are represented during a privacy debate to varying degrees. Some stakeholders may even be able to control the ability of other stakeholders to represent their interests and values. Similarly, powerful stakeholders may be able to control access to information while less powerful stakeholders may find it difficult to gain access. In the ConnectNet case the imbalance of power is evident between the Centre and sponsor companies on the one hand and privacy advocates on the other. Such an imbalance increases the risk that some privacy concerns may not be acknowledged and will not ultimately be resolved. This is highlighted in the ConnectNet case by the inability of the Centre and sponsor companies to agree with privacy advocates on the actual privacy concerns of PhysNet.

Besides the principles of representation, access, and power, two further factors became evident when analyzing the data: organizational image and timing (see Table 4). These concepts were specifically related to identifying and analyzing privacy concerns during the technology innovation process.

Organizational image (Gioia et al. 2000) can be regarded as essentially an *external view* of the organization in line with the transient impression (Berg 1985; Grunig 1993) and reputation (Fombrun 1996; Fombrun and Shanley 1990) forms of image. Image is how an external party perceives an organization, either associated with a *particular* event or action (transient impression) or *longer term* actions and achievements (reputation). How stakeholders perceive and make judgements of others is related to

Table 4. Further Concepts for Analyzing Privacy Concerns During the Innovation Process
Organizational Image • A stakeholder can use their image to legitimize their representation. • A stakeholder can use a particular image of another stakeholder to limit their representation.
Timing • The time at which a stakeholder is represented during the innovation process may affect whether they are under represented or not. • The time at which a stakeholder gains access to information during the innovation process may affect whether they can effectively deal with privacy concerns.

the image they have of others. Stakeholders are aware of the capabilities, credibility, and legitimacy of other stakeholders engaged in the privacy claims through the external image they have of these stakeholders. As was demonstrated in the analysis, the organizational image of each stakeholder was important in determining why they were considered suitable or unsuitable to represent or raise privacy claims associated with the PhysNet innovation. For example, privacy groups can legitimize their actions through their image as consumer advocates; their views on privacy are seen as aiming to protect the wider public. Industry and research organizations can question whether privacy groups should be represented during a privacy debate by presenting an image of these groups as being uninformed and against technological progress. Importantly, the power principle also affects the ability of a stakeholder to present their own image as well as a particular image of other stakeholders.

Timing: Stakeholders may be invited to represent their perspective on potential privacy risks but *when* they are invited to participate is important. This is especially relevant for privacy issues raised during technology innovation processes. If stakeholders developing technologies prefer to do so without interference, only providing access and inviting other stakeholders to represent their interests once the technology is more fully developed, there may be little opportunity to identify and deal with privacy risks. Consequently the development and adoption of such technologies may be threatened or society may face increased privacy risks. Encouraging access and representation for stakeholders with interests and values associated with a new technology earlier in the innovation process may help to identify privacy risks earlier, providing opportunities to overcome the risks in mutually beneficial ways. Alternatively, allowing representation and access too early may stifle innovation if stakeholders are unable to reach agreement on how a technology should be further developed. Stakeholders with the power to control when others are represented and when access to information is granted during the innovation process may have the ability to influence the manner in which privacy claims are dealt.

Conclusions

Technology has already had a marked impact on privacy, and will most likely continue to raise privacy concerns. It is during the innovation process that we feel significant progress can be made in ensuring that privacy claims are judged in appropriate ways. Reactions to privacy concerns during new technology development may present an early opportunity to identify privacy risks. We have provided empirical evidence for how the general principles of representation, access, and power affect how stakeholders deal with privacy. Furthermore, we have demonstrated that there are specific concepts to aid analysis of how stakeholders deal with privacy risks early on in the innovation processes. In particular, the concepts of organizational image and timing have been identified and shown to affect the way in which stakeholders deal with privacy concerns during technology development. The principles and concepts presented provide a way to evaluate how stakeholders deal with privacy concerns and in what ways these concerns are most likely to be unacknowledged or under represented. For example, power relations may be such that timely stakeholder participation is limited through constrained information flows and the representation of an unfavorable organizational image. By recognizing such situations, potentially detrimental consequences for both new innovations and privacy could be minimized. Understanding the privacy concerns of various stakeholders as well as how they deal with these concerns during the innovation process is also an important step in trying to effectively protect privacy. As we have shown in the case study, stakeholder interests are diverse, their views on privacy and how to deal with related concerns are varied. Should we try to protect and maintain levels of privacy, we need to consider strategies that ensure stakeholders are represented, access to information is granted to stakeholders, and power relationships are considered. But such strategies are also affected by the way stakeholders view each other and the timing of interactions and interventions while technologies are being developed. No single privacy management strategy would effectively deal with this complexity so a multifaceted approach is warranted. Along with the more common privacy management strategies such as legislation, self-regulation, and the use of privacy enhancing technologies, we may also have to consider less common approaches such as privacy education, technological adaptation (i.e., changing the technology to accommodate privacy concerns), and privacy trialing (i.e., conducting trials of appropriate privacy initiatives with concerned stakeholders).

References

Altman, I. *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*, Brooks/Cole Publishing Company, Monterey, CA, 1975.

Altman, I. “Privacy Regulation: Culturally Universal or Culturally Specific?,” *Journal of Social Issues* (33:3) 1977, pp. 66-84.

Bellotti, V., and Sellen, A. “Design for Privacy in Ubiquitous Computing Environments,” in *Proceedings of the Third European Conference on Computer-Supported Cooperative Work*, G. Michelis, C. Simone, and K. Schmidt (Eds.), Kluwer Academic Publishers, Boston, 1993, pp. 77-92.

Berg, P. O. "Organization Change as a Symbolic Transformation Process," in *Organizational Culture,* P. Frost, L. Moore, M. R. Louis, C. Lundberg, and J. Martin (Eds.), Sage Publications, Beverly Hills, CA, 1985, pp. 281-299.

Culnan, M. J. "Protecting Privacy Online: Is Self-Regulation Working?," *Journal of Public Policy & Marketing* (19:1), Spring 2000, pp. 20-26.

Culnan, M. J., and Armstrong, P. K. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), January-February 1999, pp. 104-115.

Culnan, M. J., and Bies, R. J. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues* (59:2) 2003, pp. 323-342.

Fombrun, C. J. *Reputation: Realizing Value from the Corporate Image*, Harvard Business School Press, Boston, 1996.

Fombrun, C. J., and Shanley, M. "What's in a Name—Reputation Building and Corporate Strategy," *Academy of Management Journal* (33:2), June 1990, pp. 233-258.

Freeman, R. E. *Strategic Management: A Stakeholder Approach*, Ballinger, Cambridge, MA, 1984.

Gavison, R. "Privacy and the Limits of Law," *Yale Law Journal* (89) 1980, pp. 421-472.

Gellman, R. "Does Privacy Law Work?," in *Technology and Privacy: The New Landscape,* P. E. Agre and M. Rotenberg (Eds.), MIT Press, Cambridge, MA, 1998.

Gerety, T. "Redefining Privacy," *Harvard Civil Rights—Civil Liberties Law Review* (12), 1977, pp. 233-396.

Gioia, D. A., Schultz, M., and Corley, K. G. "Organizational Identity, Image, and Adaptive Instability," *Academy of Management Review* (25:1), January 2000, pp. 63-81.

Grunig, J. E. "Image and Substance—From Symbolic to Behavioral Relationships," *Public Relations Review* (19:2), Summer 1993, pp. 121-139.

Hine, C., and Eve, J. "Privacy in the Marketplace," *Information Society* (14:4), 1998, pp. 253-262.

Introna, L. D., and Pouloudi, A. "Privacy in the Information Age: Stakeholders, Interests and Values," *Journal of Business Ethics* (22:1), October 1999, pp. 27-38.

Johnson, J. L. "Privacy and the Judgment of Others," *Journal of Value Inquiry* (23:2), June 1989, pp. 157-168.

Kang, J. "Information Privacy in Cyberspace Transactions," *Stanford Law Review* (50:4), April 1998, pp. 1193-1294.

Lederer, S., Dey, A. K., and Mankoff, J. "A Conceptual Model and a Metaphor of Everyday Privacy in Ubiquitous Computing Environments," Technical Report IRB-TR-02-017, Intel Research, Berkeley, CA, July 2002.

Lyon, D. *The Electronic Eye: Rise of the Surveillance Society*, Polity Press, Cambridge, England, 1994.

Marx, G. T. "Some Information Age Techno-Fallacies," *Journal of Contingencies and Crisis Management* (11:1) 2003a, pp. 25-31.

Marx, G. T. "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance," *Journal of Social Issues* (59:2) 2003b, pp. 369-390.

Parent, W. A. "Recent Work on the Concept of Privacy," *American Philosophical Quarterly* (20:4) 1983, pp. 341-355.

Pouloudi, A., and Whitley, E. A. "Stakeholder Identification in Inter-Organizational Systems: Gaining Insights for Drug Use Management," *European Journal of Information Systems* (6) 1997, pp. 1-14.

Schoeman, F. "Privacy + Philosophical Dimensions," *American Philosophical Quarterly* (21:3) 1984, pp. 199-213.

Warren, S., and Brandeis, L. "The Right to Privacy," *Harvard Law Review* (4) 1890, pp. 193-220.

Webster, J. "Desktop Videoconferencing: Experiences of Complete Users, Wary Users, and Non-Users," *MIS Quarterly* (22:3), September 1998, pp. 257-286.

Westin, A. F. *Privacy and Freedom* (1st ed.), Atheneum, New York, 1967.