POSTPRINT VERSION

The final publication is available at Springer via
http://dx.doi.org/10.1007/s00146-007-0149-7

Cite article as:

Carew, P.J., Stapleton, L. and Byrne, G.J. (2008). "Implications of an ethic of privacy for human-centred systems engineering", AI & Society 22(3), 385-403.

Implications of an Ethic of Privacy for Human-Centred Systems Engineering

Peter J. Carew, Larry Stapleton and Gabriel J. Byrne

ISOL Research Centre,
Waterford Institute of Technology,
Cork Road, Waterford, Ireland.
Tel: +353-51-302628
Fax: +353-51-302679
E-mail: pcarew@wit.ie

Abstract: Privacy remains an intractable ethical issue for the information society. Given its complicity, there is a moral obligation to redress privacy issues in systems engineering practice itself. This paper investigates the role the concept of privacy plays in contemporary systems engineering practice. Ontologically a nominalist human concept, privacy is considered from an appropriate engineering perspective: human-centred design. Two human-centred design standards are selected as exemplars of best practice, and are analysed using an existing multi-dimensional privacy model. The findings indicate that the human-centred standards are currently inadequate in dealing with privacy issues. Some implications for future practice are subsequently highlighted.

Keywords: privacy, human-centred design, best practice, Q methodology, standards, systems engineering.

1. Introduction

Privacy remains one of the most ethically imperative issues of the information age. Although the potential dangers posed to individual privacy by technological advancement have long been recognised, there are no discernible signs of the issue finding resolution. On the contrary, the unremitting development and use of systems and technologies, together with their increasingly pervasive information requirements, only serve to exacerbate the problem. Given the direct and indubitable role of contemporary technological systems in constituting many intractable privacy issues, there is a moral imperative for the matter to be revisited and redressed at source: the systems engineering process itself.

This paper considers the current role the concept of privacy plays in modern systems engineering practice. The concept of privacy is introduced to illustrate its rich meaning and considerable value for human society, and a rationale for incorporating the concept in contemporary systems engineering forwarded. Using an eclectic and multi-dimensional privacy model, two human-centred design standards are analysed and presented as a case study of best systems practice. Finally, recommendations are made to improve the incorporation of privacy in future systems engineering practice.

2. Research Objectives and Research Questions

The objective of this paper is to investigate the current role of the concept of privacy in systems engineering best practice as laid out in the human-centred design standards.

The research questions are:

1. *Does best practice for systems engineering adequately incorporate the concept of privacy?*
2. *How can the incorporation of the concept of privacy be improved in systems engineering practice?*

3. Antecedents of Privacy

3.1. Introduction to the Concept of Privacy

Privacy is an ancient Aristotelian human value (DeCew, 2002), which has in time been ascribed significant social value. References to it can be found in the great books of the world, including religious texts such as the New Testament [Matt: 6] and the Koran [24:27-28]. The concept features in diverse disciplines such as psychology, sociology, jurisprudence, politics, governance, anthropology, communications, design, and information systems. Although no universal definition exists, the famous and pervasive conception of privacy by Warren and Brandeis (1890) is "the right to be let alone."

Privacy is culturally universal, although its manifestations and associated behaviours are culturally specific (Margulis, 2003). The meaning and value of privacy varies considerably

between, and even within, social and cultural groups (Hall, 1966; Kaya and Weber, 2003). Despite its origins with the Aristotelian discourses on intimacy, there is no one definition of privacy, and there are many disagreements regarding its meaning, value and scope (DeCew, 2002). Theorists argue over whether it is a condition, a process, or a goal (Newell, 1998). There is also disagreement as to whether the value of privacy is purely instrumental or whether it is more intrinsic (Gotterbarn, 1999). Nevertheless, privacy is widely accepted to hold significant social value, and it facilitates a myriad of higher-order developmental human functions, such as creativity and personal growth (Pedersen, 1997). Privacy is also widely recognized as a fundamental human right, and is enshrined as such in numerous international covenants (cf. UN, 1948). Overall, privacy is a dynamic and amorphous concept, and one that means different things to different people.

The information systems literature has long recognised the threat posed to individual privacy by technological systems. During the early years of development in the 1970s and 1980s, the increasing use of computer systems for processing personal data, such as electronic funds transfers, raised a variety of privacy concerns (Kling, 1978). Indeed, Mason (1986) noted privacy as been one of the major ethical challenges to face the information age. It has also long been a focus of computer ethics, which involves the application of ethical theory to the use of computers and information systems (Johnson, 2001). In spite of its long-time recognition and prominence in the literature, privacy remains one of the most challenging ethical issues facing society today.

Contemporary technological development enables data practices that were previously conceivable but, until recent years, impractical (Smith, 1993). In Orwell's fictional account of a totalitarian regime in *Nineteen Eighty Four*, citizens were perpetually monitored via ubiquitous "telescreens" (Orwell, 1949). Writers such as Orwell could clearly envisage the use of omnipresent technology for endemic surveillance and control. Today, however, information and communications technologies (ICT) allow for the effortless collection, transfer, and use of more types of data in more ways than ever before. The prevalent use of technology in the information society is self-evident. It pervades all aspects of modern life, making information more accessible, and opening up applications that were previously unfeasible. Over time, such data are stored, used, and augmented to form digital "doppelgangers", describing all there is to know about us.

3.2. The Need for Privacy in Systems Engineering

There are both moral and objective imperatives to adequately incorporate the concept of privacy in all aspects of modern systems engineering. It is important to realise that privacy issues are relevant to systems engineering practice in general, and are not exclusively associated with the development and use of pure ICT or computer-based systems. The use of information technology is endemic in all industries, all professions, and all aspects of modern systems engineering, regardless of the underlying root discipline. The "informating" capabilities of automation systems for example have long been recognised as a side effect of their deployment (Zuboff, 1988), thus making any distinctions between such systems and other computer-based information systems increasingly tenuous. Systems engineering has always gathered and used data for a plethora of design, optimisation and decision-making tasks. Modern information technologies serve as tools in engineering practice for a variety of data collection, analysis, and control applications.

However, the concept of privacy is not simply concerned with the collection and dissemination of data and personal information (cf. Margulis, 2003). The concept has ancient roots that predate modern technology and systems. It has always held meaning and value with people and, therefore, any activity in the social sphere may have privacy implications and ramifications. Systems engineers must frequently deal with physical environmental issues and those people who operate in that environment. There is a plausible argument therefore, that violations of the concept of privacy occur more frequently in this domain than in pure information systems engineering, where data issues arise.

Information systems are not simply computer-based systems (Robinson et al., 1998). They also incorporate and recognise the human and social elements as pivotal in purposeful knowledge creation and transfer. This is achieved through human interactions and communications in physical or computer-mediated realities. In the workplace, this interaction depends on factors such the working environment, work practices, technological systems and tools. Systems engineering therefore always impacts on this human information system, altering its development and trajectory. There is, therefore, a need to address the engineered domain as a holistic and human-oriented system in order to avoid detrimental ramifications.

The failure rate of information systems implementation, for example, is notoriously high (Klein and Jiang, 2001), and there is subsequently an extensive literature that considers information systems success and failure factors. In general, it is recognised that many failures stem from human and organisational factors, and not technological function (Doherty et al.,

2003; Li, 1997). User resistance to technological development has long been recognised as a serious contributing factor to systems failure, and such resistance can be active or passive, overt or covert (Hirschheim and Newman, 1988).

In employee surveillance systems, for example, employees do not passively accept technologies that capture information about their whereabouts, activities or knowledge, and may use options available to them to resist, avoid and distort information gathering (Stanton and Stam, 2003). Employing intrusive systems can also deteriorate work relations and, thus, have wider indirect consequences. Mumford (2000) notes that many employees and employers have lost any feelings of mutual trust and respect, and loyalty work cultures are practically extinct. Excessive monitoring of employees will further deteriorate what remains of such relationships by implying a distinct lack of trust (Ariss, 2002).

Systems engineering that treats ethical and human values such as privacy as central issues can result in both improved systems success and reduced human ramifications such as resistance (Thomson and Schmoldt, 2001). Overall, privacy is an important and rational human concept for, and merits a discernable role in, contemporary systems engineering.

3.3. Best Practice and Privacy in Systems Engineering

3.3.1. Privacy and Systems Engineering Practice:

Privacy is frequently undervalued in systems development. Palen and Dourish (2003) note that many social and design studies of technology tend to conflate the functions and value of privacy, meaning that it is ultimately underrepresented in the engineered system. Similarly, Anton et al. (2001) argue that the software engineering community has poorly addressed privacy during systems development. In an analysis of five diverse approaches, Carew and Stapleton (2005) found that standard systems development methodologies do not consider privacy as a central issue. This problem was noted as particularly acute with those approaches that focus on the delivery of technical tools, function and artefacts.

Technology has long been used as a tool to improve efficiency and productivity. However, focusing on the instrumental value of systems to the exclusion of those people affected is morally precarious (Lyotard, 1979). An exemplar of this instrumental perspective is scientific management, or "Taylorism" (cf. Taylor, 1911). Taylorism is a totalitarian and control oriented management approach. It venerates raw efficiency, seeing nothing of value in the human aspect, and exemplifies the "man as machine" myth that has long pervaded systems

development (Hirschheim and Newman, 1991). However, the Tayloristic drive for efficiency can lead to ineffectiveness, skimping, and the unethical treatment of humans (Mintzberg, 1989). From a Tayloristic perspective, privacy is "economically inefficient" (Posner, 1978), and will therefore be ascribed little value in practice. However, there are alternatives to such approaches for systems engineering. The socio-technical approach for instance - the "antithesis of Taylorism" (Avison and Fitzgerald, 1995, p.361) - ascribes equal value to human factors and technological issues (Mumford, 2000). In this way technology can be harnessed in an effective manner, whilst respecting and empowering individual people.

Using an interesting dichotomy, Brödner and Latniak (2004) differentiate "low road" and "high road" organisational approaches. The low road approach focuses on immediate issues such as reducing expenditure, downsizing, and organisational leanness. In contrast, the high road approach recognises the benefits inherent in supporting and enabling human creativity and potential as a key to economic success. The need for employee motivation and retention as a means to retaining and expanding organisational knowledge, and the necessity of flexibility and "slack" for exploring new innovations and business opportunities, are illustrative of the high road philosophy. The concept of privacy offers notable resonance and compatibility with the high road perspective. They both value human potential, and support opportunity for autonomous creativity in ways that can ultimately be beneficial to all stakeholders beyond immediate or short-term gains. However, there appears to be some reluctance for organisations to shift from a low road to a high road approach, even through there is strong economic reason to do so (Brödner and Latniak, 2004).

In terms of systems engineering, privacy is seemingly most compatible with socio-technical approaches that incorporate human aspects, and "high road" organisational approaches that embrace the human potential in the wider system. This is logical, given that the concept of privacy is ontologically a nominalist human concept, and one that bears meaning outside of any technological implementation. One well-established tradition that merits particular attention when considering privacy in systems engineering is human-centred design.

3.3.2. Human-Centred Design and Privacy:

Human-centred design is an approach that resonates closely with the philosophy of the socio-technical approaches. The ethos of human-centred design places human considerations before those of the organisation or the technological systems being implemented (Brandt and Cernetic, 1998; Maguire, 2001). The human-centred tradition, which has strong roots in the automation literature, places human needs, purpose, skill, creativity and potential at the heart

of human organisations and technical systems design (Gill, 1996). Human-centred systems are thus created to complement human skill and to serve human needs for information, assistance and knowledge (Kling and Star, 1998).

Human-centred system design recognises that computer systems structure social relationships and not just information. The individual worker is an integral member of the wider society, and not just an isolated organisational component (Gill, 1996). Human centred systems design should be ecological, thus accounting for the holistic system development, use, infrastructure, global concerns and environmental issues (Kling and Star, 1998).

Although the ideologies of human-centred design and privacy are not identical, they appear to be highly compatible on a number of levels. For example, they are both concerned with the physical environment, individuals and social groups, society and culture, communications and cooperation between individuals and groups, individual needs and personal characteristics. Brandt and Cernetic (1998) note that people have intrinsic needs, and that these should be supported by human-centred systems. Examples include the need for people to develop themselves, to experience challenges, be creative, have motivation, experience job satisfaction, and have ample opportunity to use their tacit knowledge, ingenuity and skills. These needs map closely to a number of the higher-order functions of privacy, including personal growth, creativity, autonomy, rejuvenation, contemplation and emotional release (cf. Pedersen, 1997). The human-centred design and the philosophy of privacy approaches recognise the inherent value in allowing people to realise intrinsic and personal needs. These human needs may not be directly related to the technical system or context, but instead contribute on a wider level by enabling better use, transfer and deployment of knowledge and skill.

3.3.3. International Standards and Best Practice:

There are a plethora of methodological approaches for systems engineering (Avison and Fitzgerald, 1995). Each approach takes a different perspective on what are deemed to be rational system objectives, and each offer unique process descriptions. Some design approaches are inherently flexible, but sometimes to a degree that they offer little firm guidance on the actual process itself (Asaro, 1999). The existence of this "methodological jungle", and the fact that many organisations adopt ad hoc approaches (Avison and Fitzgerald, 2003), suggest that identifying a firm consensus on explicit "best practice" is unlikely in such an environment.

International standards on the other hand for human-centred systems design describe best practice in many areas, including best practice for ethical systems engineering. In recent years, there has been a marked increase in the use of the ISO international standards or publications as a way of establishing consensus on various aspects of systems methodology. For instance, the now ubiquitous Unified Modelling Language (UML) was established as an ISO standard in 2005 (ISO/IEC 19501). Although UML is not a development methodology in itself, but rather a graphical modelling notation, it has become a pervasive tool for systems design under the object-oriented paradigm. Similarly, the Z ("Zed") mathematical notation for formal systems specification was established as an ISO standard in 2002 (ISO/IEC 13568).

Although a variety of ISO standards consider privacy to varying degrees, there is no dedicated international standard for privacy itself (Bennett, 1997, 2000). There are, however, a number of influential privacy guidelines that currently represent international consensus on issues of informational privacy (cf. Gellman, 2002). Among the best known of these are the OECD Guidelines (OECD, 1980), and the Fair Information Practices (FIPs) (DHEW, 1973). These privacy guidelines remain influential, and offer explicit guidance on data practices for information systems engineering. However, some authors have questioned the sufficiency of the FIPs (Clarke, 1999) and the OECD Guidelines (van Wel and Royakkers, 2004) due to the new challenges brought by more recent technological innovation. Although there were some efforts at establishing an ISO privacy standard in the late 1990s, this met with considerable disagreement among national standards agencies, and the effort ultimately failed (Bennett, 2000). All international efforts have focussed on informational or data privacy, and this arguably overlooks the wider impact of pervasive technologies on the physical and social environments.

4. Case Study: Human-Centred Design Standards

A case study of two ISO human-centred design standards is presented in order to address the question "Does best practice for systems engineering adequately incorporate the concept of privacy?" These standards embody international consensus and maturity on best practice in human-centred design (Earthy et al., 2001), which is philosophically and ideologically compatible with the human concept of privacy. The first research question will be addressed by testing the single proposition:

Proposition 1. The international human-centred design standards adequately incorporate the concept of privacy.

There are a number of international standards for designing human-centred systems (cf. Jokela, 2002; Jokela et al., 2003; Maguire, 2001). This case study refers to two representative standards which have been chosen for systematic and detailed analysis, namely:-

(A) ISO 13407 (1999) – Human centred design processes for interactive systems

(B) ISO TR 18529 (2000) – Human centred lifecycle process descriptions

The ISO 13407 standard describes how a human-centred design process can be used to achieve usable systems by providing a supplementary framework to existing lifecycle models. It prescribes five key iterative processes to incorporate usability requirements into the systems development process. ISO 13407 specifies types of activities to be performed during system development without recommending particular methods or techniques (Bevan and Curson, 1999).

The closely related ISO TR 18529 standard - formally a "technical report" - identifies seven human-centred design processes, each with a purpose statement and a set of base practices (Jokela, 2002). These processes focus heavily on stakeholders, tasks, the organisation and the physical environment. It improves on ISO 13407 by considering the system in a wider context.

Overall, standards for human-centred design such as ISO 13407 and ISO TR 18529 can be used to supplement the systems development process (Bevan and Curson, 1999; Earthy et al., 2001; Maguire, 2001)..

4.1. Privacy Analysis Model

The case study will use the privacy framework model originally described in Carew and Stapleton (2005). This taxonomic model conceptualises privacy as four primary dimensions: physical, social, psychological and informational. The physical dimension is concerned with the environment, where a person may desire physical solitude. The social dimension is concerned with communications and interactions with others, and the autonomy enjoyed by individuals therein. The psychological dimension is associated with the social dimension, but

is instead concerned with the individual person and their psyche. Finally, the informational dimension is concerned with the control and dissemination of personal information.

The model amalgamates and classifies a wide range of privacy factors, which were identified through a multi-disciplinary literature review. Each factor is classified as a type, a function, or a contributing factor. A type is a form or state of privacy desired, a function is an instrumental reason why a person might seek privacy, and a contributing factor is something that has influence over a person's ability to achieve privacy. Some contributing factors are identified as being primarily local to one of the four privacy dimensions, whereas others are global and have significance across all dimensions. Table 1 (Appendix A) lists and classifies all the privacy factors of the original model.

The privacy model demonstrates that the concept of privacy can extend beyond informational issues to also include physical and social aspects. This again illustrates why systems engineers in general, and not just those concerned with information systems, must be conversant and sensitive to the range of privacy issues inherent in any given context or domain.

4.2. Methodology

The case study analysis of the human-centred design standards will use the same content analysis methodology as Carew and Stapleton (2005), which analysed five divergent systems development methodologies. Each standard's text is analysed in full, and those sections that seem to be potentially for or against specific privacy factors in the model are noted. The results of the analysis are presented in Table 1 (Appendix A) as factor-wise potentials. It is important to note that it is possible for a section or aspect of a standard to potentially be both for and against a particular privacy factor, depending on interpretation. As neither standard has been written from a privacy perspective, even alluding references to similar or related concepts have been included in the analysis to achieve a representative fairness.

4.3. Analysis Results

The analysis of ISO 13407 using the model demonstrates that privacy is not explicitly considered by the standard in any substantial way. Although a number of the privacy factors appear to have been addressed to some degree, as is evident from the positive potentials in Table 1 (Appendix A), these are frequently counterbalanced with at least as many negative

potentials. Only the environmental, organisational, and societal aspects appear to attract reasonable coverage. However, no textual reference involved privacy-specific terms, and many factors are seemingly overlooked. While the ergonomics of the physical environment are a major theme in the standard, physical privacy is not addressed beyond this.

The potentially intrusive nature of interacting with and involving users in the overall systems engineering process appears to have also been overlooked in some respects. For instance, investigating existing work practices, environment, skills, characteristics and abilities may have serious privacy ramifications. Also of note is the fact that stakeholder territoriality is inadequately managed. This territoriality or ownership may be actual or perceived, and could include physical systems or artefacts, current status, and personal knowledge and information. Such wards or territories are jealously guarded (Hart, 1994), and practices that infringe on them may be deemed intrusive. Privacy issues concerning territoriality may be particularly acute in human-based domains such as healthcare (Carew and Stapleton, 2005a).

The ISO TR 18529 standard principally builds on ISO 13407 by providing a more formal and structured set of human-centred processes. The analysis shows that ISO TR 18529 also does not specifically address issues of privacy, and that there are numerous similarities with the ISO 13407 results. In general, with one notable exception, all the weaknesses identified for ISO 13407 remain. However, the ISO TR 18529 standard more explicitly deals with the stakeholders involved in the process. Thus, the territoriality concerns are lessened, even if specific concerns are not explicitly addressed. While ISO TR 18529 is seemingly an improvement over ISO 13407 in terms of privacy, either sufficiently considers or addresses the concept. This is an important finding, especially given the seeming compatibility of privacy with the ethos of the human-centred approach.

Two human-centred standards, although still deficient in regard to the concept of privacy, generally surpass the privacy content analysis of the three soft, or socio-technical, methodologies outlined in Carew and Stapleton (2005), namely the Soft Systems Methodology (SSM), Multiview, and ETHICS. The standards evidently offer more explicit coverage than the methodologies on issues of the environment, some aspects of territoriality such as property and knowledge, intimacy, and creativity. The standards and methodologies offer similar coverage on organisational issues, personal growth, personal characteristics, status, and self-identity. However, unlike the methodologies, the standards demonstrated a patently negative potential on issues of autonomy, control, solitude, anonymity, and informational privacy in general. This is significant, as one of the most prevalent privacy theories focuses on issues of control (cf. Altman, 1976). The human-centred design processes

described by the standards may, therefore, potentially be deemed intrusive and a violation of privacy by those people affected.

4.4. Limitations of Analysis and Critique

There are some limitations to the analysis presented, and the critique of the standards must be placed in context. In focussing on the textual content of the standards, the ethos of the wider human-centred approach itself is somewhat conflated. Neither the standards nor human-centred design itself actually preclude the incorporation of privacy issues in systems engineering. The ISO 13407 standard states that it is "complementary to existing design methods and provides a human-centred perspective that can be integrated into different forms of design process in a way that is appropriate to the particular context" (p.3). It provides guidance for human-centred design, describing issues such as usability at an abstract level of principles, planning and activities (Jokela et al., 2003). The inherent and necessary flexibility in the human-centred standards is therefore acknowledged. It is recognised also that there have previously been difficulties in trying to encapsulate the concept of privacy in international standards (Bennett, 2000).

5. Findings

Proposition 1 is rejected. The international human-centred design standards do *not* adequately incorporate the concept of privacy. Consequently, the answer to the research question is simply "no". Although the standards engage with many factors of the privacy model, many others factors are overlooked or underrepresented. The fact that the word "privacy" is not included, or the concept directly addressed, in the text of either standard is of particular concern. Also, the standards appear to undervalue individual autonomy and control, which are the very edict of Altman's influential privacy model (Altman, 1976).

However, the standards must be commended in that they collectively appear to provide a greater coverage of the privacy model than the socio-technical methodologies, which themselves offer greater coverage than the technically oriented approaches (cf. Carew and Stapleton, 2005). The human-centred standards, therefore, seem to describe systems practice that is most conductive to the concept of privacy. They simply do not go far enough. Overall, it is reasonable and fair to conclude that privacy is not explicitly addressed and is,

therefore, currently underrepresented in the human-centred design standards. Accordingly, it is inadequately incorporated in systems engineering best practice.

6. Implications

In general, both the emergence of the human-centred tradition (cf. Gill, 1996) and the establishment of the human-centred standards are positive developments in incorporating human aspects, such as privacy, into mainstream systems design. However, the analysis presented by this paper demonstrates that the human-centred standards are currently inadequate in addressing issues of privacy in systems engineering and an important question is research question 2, namely:-

> "How can the incorporation of the concept of privacy be improved in systems engineering practice?"

As a first suggestion, the human-centred standards could be revised to more completely and explicitly address issues of privacy. However, difficulties were previously encountered when attempting to create an ISO standard for data privacy issues (cf. Bennett, 2000). These difficulties may be reencountered in incorporating the concept of privacy into the human-centred standards, and could prove even more acute for the wider social and environmental perspective of privacy required. However, more explicit treatment of privacy in the standards would at least remind systems engineers of its importance in any systems activity.

A second approach would be to harness the flexibility and autonomy inherent in modern systems practice in order to incorporate privacy at the level of the individual systems engineer. In some areas of systems engineering, there is an ostensible trend towards a rapid and lightweight development style that is largely devoid of formal documentation and detailed procedure. In software engineering, for instance, there is evidence that formal methodologies are not slavishly used in practice (Ovaska, 2005), and that organisations frequently use ad hoc or in house approaches (Avison and Fitzgerald, 2003). Formal planning is also being minimised in many cases. Agile approaches, for example, attempt to minimise project documentation, and iterative lifecycles often necessitate immediate technical development (cf. Abrahamsson et al., 2003).

As contemporary systems engineering practice becomes highly iterative, informal, flexible and adaptable, a compelling argument can be made: the onus of decision-making is being increasing placed on the individual systems engineer. Without detailed formal planning and guidance, how the system evolves, and what it eventually results in, is becoming more dependent on a small number of people: the engineers themselves. Thus, trust and responsibility are being placed with just a few "great designers" (Robinson et al., 1998), and the decisions they make. Even where methodological support is used, many abstract principles and ideals, such as "participative design", offer little more than "rhetoric and motive" (Asaro, 1999) to the process. They remain open to interpretation by the individual systems engineers involved.

Similarly, the inherent flexibility and abstractness of the human-centred standards leaves many aspects of it open to interpretation (cf. Jokela et al., 2003). This flexibility is not necessarily a weakness, as it allows for the standards to be deployed in any given design process or context. However, it also means that decisions regarding how to interpret and use the standards rest largely with the systems engineers themselves. In the analysis presented in Table 1 (Appendix A) a number of privacy factors simultaneously hold positive and negative potential. Which privacy potential is realised depends on how aspects of the standards are interpreted and mobilised by the systems engineers, and how the affected stakeholders perceive the results. Because of the individual influence potentially exerted by systems engineers during the systems engineering process, privacy may be most effectively incorporated through a suitable mode of professional ethics.

6.1. Professional Ethics

The systems engineering process involves ethically pertinent decision-making, and those involved would be wrong to deem their actions as being ethically neutral (Wood-Harper et al., 1996). Walsham (1993), for instance, highlighted the need for systems engineers to act as "moral agents" during systems development. By adopting professional ethics, and taking a moral stance on privacy issues, for instance, professional engineers could help curtail the development of intrusive and unethical systems and practices.

Professional ethics concerns the application of ethical theory to the workplace (Johnson, 2001). There are a variety of ethical theories, but the classical consequentialist and deontological perspectives are pervasive. In determining the moral integrity of any action, consequentialist ethics consider only the consequences, and deontological ethics consider only the actions themselves. As a result, a given action may be deemed morally sound by one

theory, but immoral by the other. There are, therefore, clear and irreconcilable tensions between these two classical perspectives (Walsham, 1996). However, alternative ethical theories have been forwarded such as Virtue Ethics (VE).

Virtue ethics focuses on moral character development and disposition, instead of relying on strict ethical rules or duties to inform personal action (Johnson, 2001). It seeks to identify, espouse, promote, and develop characteristics associated with what would be widely considered to be a virtuous person. It essentially promotes virtues that should always be followed in practice, and a deed is only considered ethical if a virtuous person would have acted likewise. Thus, moral action is action in imitation of the truly virtuous. A familiar example of virtue ethics in modern life is evident in the popular American Christian adage "What Would Jesus Do?" (WWJD). This pervasive dictum serves to remind Christians to always behave in imitation of Jesus, who is infallibly virtuous. The concept of virtue ethics has found some support in the information systems literature, where the need for developing the moral character of systems professionals is recognised as a potential practical and effective way of promoting ethical systems development (Gotterbarn, 1999a; Grodzinsky, 2000). This approach accepts and embraces the fact that personal values inform personal action on a practical level, and that impacting the underlying moral dispositions can influence these actions themselves.

Systems engineers make a number of choices that significantly affect the engineering process and its outcomes, and these choices depend heavily on personal values (Kumar and Bjorn-Andersen, 1990). People similarly rely heavily on their personal belief systems in making ethically pertinent decisions (Kreie and Cronan, 2000), a fact acknowledged by the moral character focus of virtue ethics. Privacy-related decisions in systems engineering, therefore, will rely heavily on the privacy value systems of those making them: the professional systems engineers. Although there is literature on the ethical attitudes of systems professionals (Davison et al., 2006) and their ethical decision-making processes (O'Boyle, 2002), there is little research that considers privacy specific attitudes and behaviour. These privacy attitudes must be explicated to better understand the moral rationality underpinning privacy related decision-making.

There is, however, another fundamental conundrum to consider. As the concept of privacy is amorphous and individual, different systems engineers may have different conceptions of what privacy is. Thus, the privacy values held by individual engineers may affect how privacy is incorporated in a given system's design process. It is therefore necessary to know more about the beliefs and attitudes these individual professionals bring, by way of their

personal lives, to their work practices (Probert, 2004). Overall, there is a need to understand and benchmark privacy attitudes and dispositions in immediate system contexts.

6.2. Benchmarking Privacy in Systems Engineering

The desire for privacy varies with context and culture, and from person to person (Hall, 1966; Kaya and Weber, 2003; Newell, 1998). Overall, it means different things to different people. Given the amorphous nature of privacy, any attempts to encapsulate it into a prescriptive or universal model appear almost bound to fail. The concept of privacy, therefore, needs to be understood and benchmarked in particular contexts. For systems engineering, there is an onus to look beyond informational or data privacy to also consider the physical, social and psychological aspects affected by the engineering process.

There is both a moral imperative to respect the privacy of individuals when implementing a system, and also an objective rationale to avoid harmful ramifications such as user resistance. Therefore, there is a need to uncover the privacy dispositions of individual users and other affected stakeholders, but in an unobtrusive and respectful manner. Since systems engineers use their personal value systems in decision-making (Kreie and Cronan, 2000; Kumar and Bjorn-Andersen, 1990), it would be worth understanding their attitudes and perspectives on issues of privacy.

6.3. Q Methodology

One potential approach to investigating these stakeholder and engineer privacy attitudes is through Q methodology (cf. Dos Santos and Hawk, 1988). Q methodology is a "systematic and rigorously quantitative means for examining human subjectivity" (McKeown and Thomas, 1988, p.7). It combines the individual strengths of quantitative and qualitative research approaches to reveal the subjectivity involved in any situation (Brown, 1996). Q methodology provides a mechanism for identifying different factions of opinion on any topic. Participants are presented with a set of statements to sort based on their own perceptions. The sort is relative, and normally restricted to a normal distribution. These statements are carefully selected from the wider concourse, which is "the flow of communicability surrounding any topic" (Brown, 1993, p.94). Based on the sort results, all participants are subsequently correlated to each other as whole individuals, as opposed to reducing them to a series of traits or variables. From this correlation, a series of factors are extracted that represent underlying commonalities, clusters, or factions or opinion among the participants.

7. Conclusions

Philosophically, human-centred design demonstrates exceptional resonance with the concept of privacy, and evidently more so than any other systems methodology or approach. However, taking the international human-centred standards as indicative of best practice for systems engineering, the concept of privacy is currently underrepresented therein.

In spite of this finding, both the human-centred tradition and the international standards represent practice that is innately conducive to incorporating privacy in systems engineering. There is essentially a need to make privacy issues more explicit in the prescriptive aspects of the human-centred approach. Also, the human-centred approach appears to follow the contemporary trend for flexible and adaptive systems development. This development strategy, which favours bespoke or minimal methodology, requires a considerable autonomy to reside with individual engineers or small teams when developing systems. Given the degree of personal influence individual systems engineers can potentially exert over the process and the consequent system, it may be possible for human issues such as privacy to be effectively promoted and incorporated at this individual level.

There is also a need to more fully understand the concept of privacy in the context of systems engineering from both stakeholder and engineer perspectives. Q methodology is suggested as a possible means to achieving such a rich and contextual understanding in an exceptionally unobtrusive way.

Privacy is an ancient human value that, perversely, seems to have become a contemporary problem for the information society. There is a moral obligation for the architects of the technological age, the systems engineers, to challenge this fallacy though a professional "ethic of privacy". The human-centred approach offers a particularly attractive, and ideologically compatible, foundation for future research and practice in this field.

Appendix A

Table 1. Privacy Analysis of ISO 13407 and ISO TR 18529

Dimension	Aspect	Class	ISO 13407	ISO TR 18529
Physical	Environment	Type	++++ / -	++++
	Territoriality (Property)	Type	++ / --	+++ / -
	Territoriality (Body)	Type		
	Solitude (Physical)	Type	---	---
	Repose	Type	+	
	Physical Access	Contributing Factor	--	
	Sensory and Communication Channels	Contributing Factor	-	
	Violator (Humanness and Relationship)	Contributing Factor	--	
Social	Intimacy (External)	Type		-
	Intimacy (Internal)	Type	+++ / ---	+++ / ---
	Territoriality (Status)	Type	+ / -	+++ / -
	Solitude (Social)	Type	--	---
	Anonymity	Type	---	----
	Autonomy	Type	--	-
	Interactions and Communications	Contributing Factor	++ / ---	+ / ---
	Units	Contributing Factor	+ / --	+ / -
	Formality	Contributing Factor	+ / -	+ / -
	Personalness of Topic	Contributing Factor	+	
Psychological (Functions)	Self-Identity	Function	++	++
	Personal Growth	Function	++	+++
	Autonomy	Function	--	-
	Contemplation	Function		
	Self-Protection	Function	+ / -	+
	Confiding	Function		
	Emotional Release	Function		
	Rejuvenation	Function		
	Creativity	Function	++ / -	++
Informational	Territoriality (Knowledge)	Type	---	+++ / -
	Reserve	Type	--	--
	Release of Personal Information	Contributing Factor	+ / --	-
	Distribution of Personal Information	Contributing Factor	--	-
	Use of Personal Information	Contributing Factor	--	-
Global	Control	Contributing Factor	+ / ---	+ / ---
	Personal Characteristics and Circumstance	Contributing Factor	+ / --	+++ / --
	Organisational	Contributing Factor	+++	+++
	Cultural	Contributing Factor	+	+
	Societal	Contributing Factor	++	++

Positive Potential: ++++ (Very Strong), +++ (Strong), ++ (Some), + (Weak)
Negative Potential: ---- (Very Strong), --- (Strong), -- (Some), - (Weak)

Bibliography

Abrahamsson, P., Warsta, J., Siponen, M. T., and Ronkainen, J. (2003). *New directions on agile methods: a comparative analysis.* Paper presented at the 25th International Conference on Software Engineering, Portland, Oregon.

Altman, I. (1976). Privacy: A Conceptual Analysis. *Environment and Behavior, 8*(1), 7-29.

Anton, A. I., Earp, J. B., Potts, C., and Alspaugh, T. A. (2001). *The role of policy and stakeholder privacy values in requirements engineering.* Paper presented at the Fifth International Symposium on Requirements Engineering (RE'01).

Ariss, S. S. (2002). Computer monitoring: benefits and pitfalls facing management. *Information & Management, 39*(7), 553-558.

Asaro, P. M. (1999). *Transforming Society by Transforming Technology: The Science and Politics of Participatory Design.* Paper presented at the Critical Management Conference, Manchester.

Avison, D. E., and Fitzgerald, G. (1995). *Information Systems Development: Methodologies, Techniques and Tools* (2nd ed.). London: McGraw-Hill.

Avison, D. E., and Fitzgerald, G. (2003). Where now for development methodologies? *Communications of the ACM, 46*(1), 79-82.

Bennett, C. J. (1997). Arguments for the standardization of privacy protection policy: Canadian initiatives and American and international responses. *Government Information Quarterly, 14*(4), 351-362.

Bennett, C. J. (2000). *An international standard for privacy protection: objections to the objections.* Paper presented at the Tenth conference on computers, freedom and privacy, Toronto.

Bevan, N., and Curson, I. (1999). Planning and implementing user-centred design. *CHI '99 extended abstracts on Human factors in computer systems*, 137-138.

Brandt, D., and Cernetic, J. (1998). Human-centred approaches to control and information technology: European experiences. *AI & Society*(12), 2-20.

Brödner, P., and Latniak, E. (2004). Recent findings on organisational changes in German capital goods producing industry. *Journal of Manufacturing Technology Management, 15*(4), 360-368.

Brown, S. R. (1993). A primer on Q methodology. *Operant Subjectivity, 16*, 91-138.

Brown, S. R. (1996). Q Methodology and Qualitative Research. *Qualitative Heath Research, 6*(4), 561-567.

Carew, P. J., and Stapleton, L. (2005). Towards a privacy framework for information systems development. In O. Vaselicas, W. Wojtowski & G. Wojtowski (Eds.), *Information Systems Development: Advances in Theory, Practice and Education* (pp. 77-88): Kluwer Academic Press / Plenum.

Carew, P. J., and Stapleton, L. (2005a). *Privacy, patients and healthcare workers: a critical analysis of large scale, integrated manufacturing information systems reapplied in health.* Paper presented at the 16th IFAC World Congress, Prague.

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

Davison, R. M., Martinsons, M. G., Lo, H. W. H., and Kam, C. S. P. (2006). Ethical values of IT professionals: evidence from Hong Kong. *IEEE Transactions on Engineering Management, 53*(1), 48-58.

DeCew, J. (2002). Privacy. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy* (Summer 2002 ed., pp. Online).

DHEW. (1973). *Records, Computers, and the Rights of Citizens*: US Department of Health, Education, and Welfare.

Doherty, N. F., King, M., and Al-Mushayt, O. (2003). The impact of inadequacies in the treatment of organizational issues on information systems development projects. *Information & Management, 41*(1), 49-62.

Dos Santos, B. L., and Hawk, S. R. (1988). Differences in analyst's attitudes towards information systems development: Evidence and implications. *Information & Management, 14*(1), 31-41.

Earthy, J., Sherwood Jones, B., and Bevan, N. (2001). The improvement of human-centred processes—facing the challenge and reaping the benefit of ISO 13407. *International Journal of Human-Computer Studies, 55*(4), 553-585.

Gellman, R. (2002). Perspectives on privacy and terrorism: all is not lost—yet *Government Information Quarterly, 19*(3), 255-264.

Gill, K. S. (1996). The human-centred movement: the British context. *AI & Society, 1996*(10), 109-126.

Gotterbarn, D. (1999). Privacy lost: The Net, autonomous agents, and 'virtual information'. *Ethics and Information Technology, 1*(2), 147-154.

Gotterbarn, D. (1999a). Two Approaches to Computer Ethics. *SIGCSE Bulletin, 31*(2), 11-12.

Grodzinsky, F. S. (2000). The Development Of The 'Ethical' ICT Professional. *Computers and Society*(March), 3-7.

Hall, E. T. (1966). *The Hidden Dimension*. New York: Doubleday.

Hart, D. N. (1994). *On Organizations, Enterprise-Wide Information Systems and End-User Computing*. Paper presented at the 5th Australasian Conference on Information Systems, Monash University, Melbourne.

Hirschheim, R., and Newman, M. (1988). Information systems and user resistance: theory and practice. *The Computer Journal, 31*(5), 398-408.

Hirschheim, R., and Newman, M. (1991). Symbolism and information systems development: myth, metaphor and magic. *Information Systems Research, 2*(1), 29-62.

Johnson, D. G. (2001). *Computer Ethics* (International ed.). NJ: Prentice Hall.

Jokela, T. (2002). Making user-centred design common sense: striving for an unambiguous and communicative UCD process model. *Proceedings of the second Nordic conference on Human-computer interaction*, 19-26.

Jokela, T., Iivari, N., Matero, J., and Karukka, M. (2003). The standard of user-centered design and the standard definition of usability: analyzing ISO 13407 against ISO 9241-11. *Proceedings of the Latin American conference on Human-computer interaction*, 53-60.

Kaya, N., and Weber, M. J. (2003). Cross-cultural differences in the perception of crowding and privacy regulation: American and Turkish students. *Journal of Environmental Psychology, 23 (Sept 2003)*(3), 301-309.

Klein, G., and Jiang, J. J. (2001). Seeking consonance in information systems. *Journal of Systems and Software, 56*(2), 195-202.

Kling, R. (1978). Value conflicts and social choice in electronic funds transfer system developments. *Communications of the ACM, 21*(8), 642-657.

Kling, R., and Star, S. L. (1998). Human centered systems in the perspective of organizational and social informatics. *ACM SIGCAS Computers and Society, 28*(1), 22-29.

Kreie, J., and Cronan, T. P. (2000). Making ethical decisions. *Communications of the ACM, 43*(12), 66-71.

Kumar, K., and Bjorn-Andersen, N. (1990). A cross-cultural comparison of IS designer values. *Communications of the ACM, 33*(5), 528-538.

Li, E. Y. (1997). Perceived importance of information system success factors: A meta analysis of group differences. *Information & Management 32*(1), 15-28.

Lyotard, J.-F. (1979). *The Postmodern Condition: A Report on Knowledge*. Manchester: Manchester University Press.

Maguire, M. (2001). Methods to support human-centred design. *International Journal of Human-Computer Studies, 55*(4), 587-634.

Margulis, S. T. (2003). On the Status and Contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues, 59*(2), 411-unknown.

Mason, R. O. (1986). Four Ethical Issues of the Information Age. *MIS Quarterly, 10*(1), 5-12.

McKeown, B., and Thomas, D. (1988). *Q Methodology*. Newbury Park CA: Sage.

Mintzberg, H. (1989). *Mintzberg on Management: Inside Our Strange World of Organisations*. NY: The Free Press.

Mumford, E. (2000). A socio-technical approach to systems design. *Requirements Engineering, 5*, 125-133.

Newell, P. B. (1998). A cross-cultural comparison of privacy definitions and functions: A systems approach. *Journal of Environmental Psychology, 18*(4), 357-371.

O'Boyle, E. J. (2002). An ethical decision-making process for computing professionals. *Ethics and Information Technology, 4*(4), 267-277.

OECD. (1980). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

Orwell, G. (1949). *Nineteen Eighty-Four*. London: Penguin.

Ovaska, P. (2005). *Studies on Coordination of Systems Development Process.* Unpublished Doctoral Thesis, Lappeenranta University of Technology, Finland.

Palen, L., and Dourish, P. (2003). *Unpacking "privacy" for a networked world.* Paper presented at the Conference on Human factors in Computing Systems, Ft. Lauderdale, Florida.

Pedersen, D. M. (1997). Psychological functions of privacy. *Journal of Environmental Psychology, 17*(2), 147-156.

Posner, R. A. (1978). An economic theory of privacy. *Regulation*(May/June), 19-26.

Probert, S. K. (2004). Adorno: a critical theory for IS. In J. Mingers & L. Willcocks (Eds.), *Social Theory and Philosophy for Information Systems* (pp. 129-156). Chichester: Wiley.

Robinson, H., Hall, P., Hovenden, F., and Rachel, J. (1998). Postmodern software development. *The Computer Journal, 41*(6), 363-375.

Smith, H. J. (1993). Privacy policies and practices: inside the organizational maze. *Communications of the ACM, 36*(12), 105-122.

Stanton, J. M., and Stam, K. R. (2003). Information Technology, Privacy, and Power within Organizations: a view from Boundary Theory and Social Exchange perspectives. *Surveillance & Society, 1*(2), 152-190.

Taylor, F. (1911). *The Principles of Scientific Management*. NY: Harper.

Thomson, A. J., and Schmoldt, D. L. (2001). Ethics in computer software design and development. *Computers and Electronics in Agriculture, 30*(1-3), 85-102.

UN. (1948). United Nations Universal Declaration of Human Rights.

van Wel, L., and Royakkers, L. (2004). Ethical issues in web data mining. *Ethics and Information Technology, 6*(2), 129-140.

Walsham, G. (1993). Ethical issues in information systems development: the analyst as moral agent. In D. Avison, J. E. Kendall & J. DeGross (Eds.), *Human, Organizational, and Social Dimensions of Information Systems Development*. Amsterdam: North-Holland.

Walsham, G. (1996). Ethical theory, codes of ethics and IS practice. *Information Systems Journal, 1996*(6), 69-81.

Warren, S. D., and Brandeis, L. D. (1890). The right to privacy: the implicit made explicit. *Harvard Law Review, 4*, 193.

Wood-Harper, A. T., Corder, S., Wood, J. R. G., and Watson, H. (1996). How we profess: The ethical systems analyst. *Communications of the ACM, 39*(3), 69-77.

Zuboff, S. (1988). *In the Age of the Smart Machine: The Future of Work and Power*. New York: Basic Books.