Information Privacy in a Globally Networked Society
Implications for IS Research

Davison, Robert M.; Smith, H. Jeff; Clarke, Roger; Langford, Duncan; Kuo, Bob

Published in:
Communications of the Association for Information Systems

Published: 01/10/2003

Document Version:
Final Published version, also known as Publisher's PDF, Publisher's Final version or Version of Record

Published version (DOI):
10.17705/1CAIS.01222

Publication details:
Davison, R. M., Smith, H. J., Clarke, R., Langford, D., & Kuo, B. (2003). Information Privacy in a Globally Networked Society: Implications for IS Research. *Communications of the Association for Information Systems*, *12*, Article 22. https://doi.org/10.17705/1CAIS.01222

Communications of the Association for Information Systems

Volume 12 Article 22

9-11-2003

Information Privacy in a Globally Networked Society: Implications for IS Research

Robert M. Davison
City University of Hong Kong, isrobert@cityu.edu.hk

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

Duncan Langford
University of Kent at Canterbury, D.Langford@ukc.ac.uk

Feng-Yuan Kuo
National Sun Yat Sen University, bkuo@mis.nsysu.edu.tw

H. Jeff Smith
Wake Forest University, jeff.smith@mba.wfu.edu

Information Privacy in a Globally Networked Society: Implications for IS Research

Erratum

In May 2013, significant revisions were made to this paper, on pp. 356-359. The original version included an extensive segment of text from the book, The Forest and the Trees: Sociology as Life, Practice, and Promise, by Prof. Allan Johnson, and it failed to make clear which parts of the text were original and which were from Johnson. This version corrects that error, by substituting text that makes use of Johnson's ideas rather than his text directly, but retains a particularly significant quotation. The authors have apologized to the Editor of CAIS and to Prof. Johnson for the inappropriate use of the segment of text.

Communications of the Association for Information Systems

Volume 12, Article 24
October 2003

INFORMATION PRIVACY IN A GLOBALLY NETWORKED SOCIETY: IMPLICATIONS FOR IS RESEARCH

Robert M. Davison
City University of Hong Kong
isrobert@cityu.edu.hk

H. Jeff Smith
Wake Forest University

Roger Clarke,
Xamax Consultancy Pty Ltd, Australia

Duncan Langford
University of Kent at Canterbury, United Kingdom

Bob Kuo
National Sun Yat Sen University, Taiwan

CORRECTION

In May 2013, significant revisions were made to this paper, on pp. 356-359.

The original version included an extensive segment of text from the book, *The Forest and the Trees: Sociology as Life, Practice, and Promise*, by Prof. Allan Johnson, and it failed to make clear which parts of the text were original and which were from Johnson.

This version corrects that error, by substituting text that makes use of Johnson's ideas rather than his text directly, but retains a particularly significant quotation.

The authors have apologized to the Editor of CAIS and to Prof. Johnson for the inappropriate use of the segment of text.

INFORMATION PRIVACY IN A GLOBALLY NETWORKED SOCIETY: IMPLICATIONS FOR IS RESEARCH

Robert M. Davison
City University of Hong Kong
isrobert@cityu.edu.hk

H. Jeff Smith
Wake Forest University

Roger Clarke,
Xamax Consultancy Pty Ltd, Australia

Duncan Langford
University of Kent at Canterbury, United Kingdom

Bob Kuo
National Sun Yat Sen University, Taiwan

ABSTRACT

In this paper, we present an extended discussion of issues associated with the role of information privacy in IS research. This discussion was initiated in conjunction with a panel session at the Barcelona ICIS meeting in 2002. Following the conference, each of the panelists reworked and extended their position statements, and provided a commentary on the position statements of the other panelists. The paper is framed with head and tail pieces written by the panel chair. The result is a unique (and provocative) blend of opinion and commentary on a topic that is of critical importance to IS research in the globally networked society in which we all live. IS researchers will find research questions, research conundrums and research advice in equal measure.

Keywords: Information Privacy; IS Research

1.INTRODUCTION

Individual awareness of and concern for deteriorating standards of personal privacy grew steadily since the inception of modern information technology in the mid 20th century. The recent popularity of the world wide web, which significantly increases the possibility of privacy invasions by both commercial and public agencies, has further heightened people's anxiety [cf. Brendon, 2002; Liu and Arnett, 2002]. Microsoft's .Net Passport came in for particular scrutiny and was radically redesigned to avoid a clash with European regulators over privacy [Meller, 2003]. Most economically advanced countries legislated privacy protection measures in the 1970s and 1980s, even before Internet/web developments, and more are following (often precisely with ecommerce in mind), e.g. Malaysia [Azmi, 2002].

These privacy protection measures were developed in the context of trans-border data flows (TBDFs), i.e. the transfer of data across national and/or jurisdictional borders. The OECD Guidelines of 1980 are usually considered to be the primary codification of the 'Fair Information Practices' approach to privacy protection. They were explicitly driven by economic concerns rather than by a desire to protect privacy, to avoid inconsistencies between national laws creating an obstacle to trade in personal data.

Some nations and nation-groups, notably the European Union, as well as sub-national jurisdictions (such as the Hong Kong Special Administrative Region of the People's Republic of China) developed stricter legislative requirements than others with respect to TBDFs, which is important in the light of the ease with which data can be (and often needs to be) transferred. It is notable, for example, that EU firms cannot legally transfer data to organisations in jurisdictions where inappropriate (or non-existent) data protection legislation is in force. SABRE, the US-based airline reservation system, was unable to register itself in Sweden as the Swedish Data Inspectorate required the company, as a condition of

registration, to inform passengers that their flight reservation data would be transferred to the US [Scheibal and Gladstone, 2000]. In Hong Kong, similar restrictions exist, which may prove problematic for organisations like banks that outsource their data processing operations to other locations in the People's Republic of China [Fluendy, 2000]: this is less a national sovereignty issue than one of jurisdiction and protection for private data.

Perhaps unsurprisingly, there has been some criticism of this legislative trend from economists and technology proponents who argue that the traditional notion of privacy is variously outdated or obstructive to business growth, especially in the burgeoning e-business arena [cf. Liu and Arnett, 2002]. Applications such as enterprise resource planning, customer relationship management and the whole personalisation industry are dependent on a free flow of personal data in one way shape or another. Thus, it may be argued that the sharing by both individuals and business corporations of personal data is a necessary part of an efficient and effective electronic commerce.

An effective self-regulatory system has yet to emerge and so additional incentives are required in order to ensure that consumer privacy will be protected. The information sharing view may be couched in sound economic theories, but in the real world both businesses and governments have far more resources to invest in IT than ordinary people, resulting in their superiority in manipulating the system to their various advantages. For example, a key issue that underlies the current concern for protection of privacy relates to the extreme ease with which personal data, once stored electronically, can be transferred in digital format over the Internet and other networks in the globally networked society in which most of us live. Since the incremental cost of this transfer is close to zero, and since personal data is often, even if illegally, available at minimal cost, the effort required to collect, analyse and distribute such data is negligible. Consequently, while economic advantages may easily accrue to the

holders of data, data subjects may very rapidly lose any semblance of privacy, with all the resultant negative repercussions such as the torrents of spam email, cold-calling telesales, and the use of cookies that collect private data. Thus, the information privacy-related issues are evidently of immediate concerns to society and, accordingly, they should be reflected in the research conducted by IS academics.

To investigate information privacy in the globally networked society, a panel session was conducted at the 23rd International Conference on Information Systems in Barcelona, Spain [Davison et al., 2002]. The panelists themselves came from countries distributed around the world: the panel chair comes from Hong Kong, while the panelists hark from Australia, Great Britain, Taiwan and the USA. These geographically and culturally diffused societies provided the backdrop for a varied set of perspectives on information privacy and its role in IS research. The panel was purposely designed to be primarily relevant to IS researchers in general, not only those who are specialized in researching information privacy issues. Each panelist presented controversial and challenging perspectives related to the importance of information privacy in IS research. We were gratified by the enthusiastic participation of the audience, who actively waded into the debate and contributed many insights which helped stimulate the development of this paper.

The key question that was devised to motivate the discussion in this panel was as follows:

- In what ways do information privacy matters challenge IS researchers as they go about their normal business?

Following this introduction, the extended position statements of each panelist are provided. Each position statement is followed by a critique offered by one or more of the other panelists. The closing section to the article attempts to integrate the various perspectives, at the same time indicating the critical

information privacy concerns for all IS researchers as well as future research directions.

II. ROGER CLARKE'S POSITION AND PANELIST COMMENTARY

My thesis is that, in contexts in which privacy is a significant factor, research quality is extraordinarily difficult to attain. As a consequence, publication will only be achieved when fashion and topicality convince journal referees and editors to accept a paper that falls below their normal expectations.

My argument is based on the following considerations:

- quality challenges in attitudinal surveys in general:
    - measurement bias and response bias
    - non-response bias
    - proxy sampling frames
    - unjustified assumptions about Likert scales

- quality challenges in privacy-related research in particular:
    - non-response levels and biases
    - situational relativities
    - cultural relativities
    - rigour versus relevance to strategy and policy

QUALITY CHALLENGES IN ATTITUDINAL RESEARCH

Attitudinal surveys are capable of producing data whose quality is high when judged against criteria such as their amenability to powerful analytical techniques. But to the extent that quality depends on correspondence of the measures to particular real-world phenomena, the data that most surveys produce are merely fodder for exercises in statistical analysis. As training for new academics, such surveys may be justifiable, but they produce no information relevant to the real world, and should therefore fail a critical test of publishability.

Attitudinal survey design must confront many sources of uncontrollable measurement bias and response bias. The phrasing of questions creates major impacts on respondents, and the impacts vary between respondents. The sequence of questions also leads respondents to particular understandings of the meanings of words used. Questions about sensitive topics cause respondents to choose their answers carefully, with a view towards self-protection at least as much as towards honesty. The context that each respondent perceives for the questions is likely to include factors that are extraneous to the designer's intention, that may vary during the course of the data collection, and that may even be unknown to the researcher.

The notion of non-response bias refers to refusals being non-random, which is likely to result in the distribution of sample responses being different from that for the population. Yet many researchers make the implicit assumption that very similar distributions would be achieved across the responding and the non-responding groups. The non-response bias problem also arises at the level of individual questions.

Proxy sampling frames, whose characteristics are very different from those of the target population, are massively over-used. Most commonly, students are used as a convenience sample, under the pretext that the research is exploratory. Students are, in most circumstances, unrepresentative of the population that is ostensibly being researched. In many cases, they are also captive, and the proportion that answers other than honestly is likely to be high. Although some of these pseudo-responses may be easily filtered, they often are not, and some pseudo-responses are difficult to detect.

Likert scales are a commonly-used device. They usually involve very short statements, with very limited context provided that might encourage common understanding of the terms used. The lists of statements are frequently long, and

boredom-inducing. Worse still, the responses are actually qualitative, and 'category ordinal' in nature; but they are assumed to be quantitative, 'ranked ordinal' data. Some researchers then apply more powerful statistical techniques to them which are only actually applicable to data that is on a cardinal scale. It is not uncommon to do so without even discussing the possibility that the respondents did not realise that the options that were described with written words and with numbers adjacent to them were supposed to be interpreted as having equal distances between them.

QUALITY CHALLENGES IN PRIVACY-RELATED RESEARCH

Research in which privacy factors arise is yet more problematical. Such research includes not only surveys whose express purpose is to sample attitudes to privacy, but also research designs in which privacy is an intervening, moderating, or confounding variable. The involvement of privacy is frequently overlooked. For example, it is quite astonishing that a high proportion of the burgeoning literature on trust in the context of B2C fails to control for privacy, fails to meaningfully consider it, or even completely overlooks it.

The non-response bias problem is an especial challenge. It seems reasonable to assume that distributions of responses from people who are willing to answer questionnaires about privacy topics will be different from those that would arise if it were possible to obtain responses from those who decline to participate. Moreover, it would seem reasonable to assume that a significant proportion of those who decline do so because they place a high value on privacy. Hence there is likely to be a systematic bias in the data that is gathered, with the level of privacy concern in the population consistently under-stated by the respondent sample. The scale of the bias may be very substantial: in one of the rare instances in which the refusal rate is quoted, almost 4,250 people needed to be approached for every 1,000 responses achieved [OFPC 2001]. Yet discussion of this problem is almost entirely absent from conference papers and journal articles in the information systems discipline.

Among those who do provide responses, the scope for variation in the understanding of questions that involve privacy is enormous. The laws of most countries do not define the term 'privacy', because it is so highly open-textured. It has multiple dimensions, at least those of privacy of the person, of personal behaviour, of personal communications, and of personal data [Clarke 1997]. Hence respondents may make very different interpretations of the most carefully-phrased question. Yet it is unusual for researchers to provide respondents with any kind of tutorial, or even a glossary, and it is unusual to see discussions of the steps taken to overcome measurement and response bias arising from such difficulties, or to assess their impact.

Beyond the definitional aspects, people's reactions are subject to situational relativity. A person who has a current health condition that is embarrassing to them might well be more likely to place a high value on health care data relative to other data, or to other interests. A person's attitudes to the disclosure of details on a doctor's certificate supporting an employee's absence from work are likely to vary depending on whether they are interviewed in the context of their role as an employee or as a supervisor.

Some of these variations may be controllable, or sufficiently uncommon that their effects might be lost in the 'noise'. Other relativities, however, are likely to result in outright biases. Intrusiveness into the lives of pilots and train-drivers is likely to be more widely supported shortly after a plane or train crash. Media reports (which for the most part reflect propaganda, public relations campaigns and controlled information flows from governments, government agencies and corporations) are likely to condition responses during the days and weeks that follow their publication. An extreme case of this bias is evident in the enormous politicisation of privacy-related matters in the U.S.A., the U.K., and a few other countries following the assault on civil rights unleashed since 12 September

2001, and justified as responses to the terrorist assaults on New York and Washington DC the previous day.

Privacy attitudes are also subject to enormous cultural variation. For example, much of Western Europe places high value on the protection of personal data against government agencies and corporations, and regards statutory legal measures as essential. Scandinavian countries, however, especially Denmark, evidence something of a truce between data protections and openness. In the U.S.A., the public's attitudes are highly dependent on the media, and the American press is dominated by the interests of big business, and the kind of libertarian idealism that opposes government regulation and naïvely assumes that people are powerful enough to resist business and government agency intrusions. In East Asian countries, subservience to authority is highly-valued, to the extent that the Hong Kong Privacy Commissioner had to create a Zhongwen character to enable 'privacy' to be rendered in written Chinese.

Of course, the nation-state is far from an adequate proxy for culture. There is a spectrum of opinion within each country. There is a significant lingual dimension to culture. And the religio-philosophical dimension varies in its intensity from minor to determinative. The conventional Hofstede analysis appears paltry as a means of controlling for such complex patterns.

A final area of difficulty for research in domains in which privacy is a significant factor is the unwillingness of the elders of the information systems discipline to recognise relevance to public policy as a criterion. The scientific tradition demands rigour of process, and 'hard', quantitative data. Interpretivism lacks firm ground in both process and data; but it made headway during the last two decades, as the inherent ambiguity and multi-valuedness of information was accepted as a characteristic of organisational contexts. But the preference remains strong for researchers to seek explanatory and predictive power, and to

leave normative questions to other disciplines. Critical theory, with its explicit recognition of the inbuilt biases attributable to convention and to control of the public agenda by the politically powerful, is making only slow progress towards acceptability. Applied research, which applies known tools in new contexts, is acceptable. But instrumentalist research, which seeks solutions to problems, is still perceived to be 'unclean', especially where the context is public policy rather than management or strategy.

Privacy-related research evidences a combination of the least fashionable features: it deals in muddy concepts, soft data, uncertainty of process, politically-alive issues, and contentious public policy questions.

CONCLUSIONS

When privacy infects a research domain, or is expressly the topic of research, the quality that is capable of being attained is significantly lower than that which is achievable in other areas. The intrinsic quality of research can be improved by the use of techniques that provide reasonably-deep-but-reasonably-broad rather than broad-but-shallow data. Focus groups are a valuable tool for these purposes, but are shunned in academic circles. Deep research methods such as field studies and case studies are weak, however, because attitudes are so highly variable, and the applicability of outcomes is very limited without sufficient breadth to complement the depth.

Publication will be feasible in marginal conferences and journals, and in specialised conferences and journals. Publication in the mainstream of information systems depends on change in the notions of quality applied by senior editors, much greater emphasis on relevance even when at the cost of rigour, and acceptance of a focus on public policy as being as legitimate as information technology applications, management and strategy.

I argued some years ago that a researcher whose career depends on publications is well-advised not to adopt economic, legal and social implications

of information systems as their sole specialisation [Clarke 1988]. The outlook has improved only marginally during the intervening 15 years. The publication of privacy-related research will continue to depend on ingenuity and opportunism.

H. JEFF SMITH'S REACTION

Before addressing Roger's comments directly, I will provide a bit of background regarding the importance of this discussion. In the March 2002 issue of *MIS Quarterly*, Richard Baskerville and Michael D. Myers argued that IS should now be seen as a reference discipline for others, so that "scholars from many other fields look to our top journals for leadership and guidance" [Baskerville and Myers, 2002, p. 11]. In a similar vein, during the ICIS 2002 conference, Suzi Iacono argued during a panel on the "IT artifact" that IS scholars are particularly well positioned to address a number of topics associated with the process of design ➔ use ➔ implementation. In that context, it should be clear that information privacy is one topic in which IS researchers are highly suited to produce studies that fulfil the "reference discipline" criteria. By training and orientation, the match between our understanding and the issues positions us well, overall, in our quest to provide the necessary leadership and guidance. This idea becomes clear if we consider the salient domains of understanding for information privacy research.

Domains of Understanding

Four domains of understanding can be particularly relevant in information privacy research; IS researchers exhibit some level of expertise in all four.

- The "art of the possible" in IT applications
- Strategic uses of information
- Internal and external processes that drive policies and practices associated with information privacy
- An understanding of the ethical dynamics that surround information privacy issues

1. Information privacy research demands an understanding of the art of the possible in IT applications – that is, which applications can be implemented today, and which applications can reasonably be expected to emerge in the future? Computer scientists are often on the leading edge in their understanding of information technology itself and are often in an excellent position to comment on technological breakthroughs. However, it is the IS discipline that is best positioned to comment on the applications that may be enabled by these technologies, because those applications represent a marriage of real-world needs with technology.

2. Information privacy research demands an understanding of strategic uses of information – that is, the ways in which organizations leverage information to gain competitive advantage. A large percentage of the initiatives that are perceived as privacy threats were the result of an attempt by an organizational entity to harness the power of information. The academic discipline of marketing is well prepared to comment on uses of personal information for targeting (potential) customers, although many of the information uses that cause privacy concerns (e.g., employee surveillance) fall outside this zone. The academic discipline of strategy appears prepared to comment to some extent on the uses of information that change the power balance within industries or that drive significant shifts in the industry value system. However, the history of the modern academic discipline of strategy is no longer than that of the IS discipline, and the strategy discipline's development is in many senses quite fragmented. Perhaps for that reason, the earliest work on strategic information systems seemed to emerge at almost the same time from the disciplines of strategy and IS [e.g., McFarlan, 1984 and Porter, 1985] – and the development of theory in the two domains seemed to occur since then at a somewhat similar pace. Furthermore, to the extent that competitive advantage derives from realignment of the supply chain, the academic discipline of operations is especially well positioned to offer insights - although, in that context, customarily little of the information is of a personal form. Thus, as compared to other disciplines, IS since the 1980s has held its own

in its ability to explain the sources of competitive advantage from information and to offer guidance in exploiting those sources.

3. Many types of information privacy research demand an understanding of the internal and external processes that drive policies and practices associated with information privacy - that is, how policies are created and how they are implemented in actual practice. Of course, organizational behavior (OB) researchers are well placed to comment on the various factors that, within the organization, drive executives, managers, and employee behaviors, both within policy boundaries and outside of them. However, OB research generally pays less attention to the intermingling of external factors (e.g., governmental regulation, media exposure) with the internal ones. Indeed, some of the few privacy studies to examine these internal-external relationships emanated from the IS discipline [e.g., Smith, 1993; Milberg et al., 2000].

4. Some types of information privacy research - those that take normative positions about privacy[1] - demand an understanding of the ethical dynamics that surround information privacy issues - that is, how (if at all) a "right to privacy" is defended in ethical terms and which managerial duties associated with protecting that right therefore accrue. The discipline of philosophy devoted much attention to an exploration of privacy's definition and moral defense [for example, see Schoeman, 1984], but it is less precise at the more granular level of specific managerial obligations. For example, the concept of "Fair Information Practices" has been cited since 1973 by privacy advocates and some researchers as imposing a number of ethical duties on managers. However, I am unaware of any normative defense of such duties being published in the philosophy literature or, for that matter, in the IS literature. Indeed, neither of the two disciplines can claim exhaustiveness in its handling of normative privacy arguments. It is also true that

[1] Here, I distinguish between descriptive statements (about how the world is) and normative statements (about how the world ought to be or about what an entity ought to do). This concept is discussed again in the next section.

only a small percentage of IS researchers are trained in the techniques of normative philosophical argumentation that are required for rigorous handling of these issues. Even so, for the IS researchers who are, it appears that they would be fully capable of leading in this dimension of privacy research.

Thus, at least a portion of the academic discipline of IS is well qualified to lead in gaining understanding within all four of these areas, which suggests that information privacy is indeed a viable domain in which IS could become a reference discipline. Yet Roger seems to suggest that we should forfeit this opportunity and adopt a fatalistic perspective regarding the concept of privacy research. Why would there appear to be such a problem with doing privacy research - and can we address this problem?

A Problem with Privacy Research?

The best approach to evaluating approaches to privacy research is to consider the different ways in which such research *might* be conducted. Although in no way unique to privacy issues, a general framework for research can be constructed by accepting philosophy's distinction between descriptive and normative statements. Descriptive statements — those that say something about how the world *is* — are quite different from normative statements, which prescribe how the world *ought* to be or what an entity (human or otherwise) *ought* to do.

Normative arguments about privacy are produced most often by philosophers and, in their journals' editorial processes, are subjected to the rigorous scrutiny of the discipline. For example, a philosopher might write a treatise that defended the existence of a "right to privacy". The editorial process would ensure that the author's premises were stated and defended, that assumptions were clarified and defended, and that conclusions were drawn through a rigorous process. The author would be expected to call out and answer likely objections to his or her argument. Such a treatise would not be expected to address research design, sampling procedure, data analysis, and the like, since they mean little in the domain of normative argumentation. In fact, to the extent that data from the real

world were mentioned in the treatise, they would be included solely to further the ethical argumentation.

On the other hand, within the category of descriptive research[2], it is critical to understand relationships within the real world. This category can be subdivided by considering the type of understanding to be furthered. Lee [1991] called out three types of such understanding:

- Subjective understanding – understanding that belongs to human subjects in some setting. The subjects use common sense and their own terminology to understand themselves, their setting, and their own behaviors within that setting;
- Interpretive understanding – understanding that belongs to a researcher as s(he) interprets the subjective understanding, often by using such methods as rich field-based methods, ethnography, or action research, and
- Positivist understanding (also called scientific theory) – understanding that belongs to a researcher as (s)he follows the scientific method in formulating and testing hypotheses. When accumulating positivist understanding, a researcher uses constructs that belong exclusively to him or her – not to the human subjects. (For example, human subjects would not understand the construct "locus of control", but the researcher might use that construct in testing a hypothesis).

Lee [1991] argues that these three forms of understanding reinforce one another in a continuous loop so that, for example, increased interpretive understanding would then lead to more informed hypotheses for positivist tests. For our

[2] A source of minor confusion is that social scientists sometimes use the word "descriptive" in a different way. Studies that do not test theory but that simply report demographic data are sometimes called "descriptive," but that is not the use of the word intended here. Throughout this discussion, the word "descriptive" is used in the philosophical sense.

purposes, the most important point is that all three of these forms of understanding come under the rubric of descriptive, rather than normative, research.

Researchers considering issues associated with privacy might profitably embrace either:

- normative argumentation, in which case their work would be subject to the rules of rigor associated with the discipline of philosophy,
- descriptive research whose goal is interpretive understanding of a privacy-related phenomenon, in which case their work would be subject to the rules of rigor associated with interpretive research, or
- descriptive research whose goal is positivist understanding of a privacy-related phenomenon, in which case their work would be subject to the rules of rigor associated with positivist research.

Since subjective understanding is held by the human subjects rather than researchers, it is not a candidate.

All of these approaches to privacy research can indeed be successful when handled with appropriate levels of rigor[3]. However, two potential problem areas may limit the ability to publish privacy research in the top outlets. First, and quite obviously, one can attempt research in any of these categories but perform it sloppily. For example, one might attempt a study with an objective of positivist understanding, but with weak theoretical development and poorly constructed measures. Such a paper would rarely be accepted for publication by a top outlet. There is no reason to believe that such sloppiness is any more inherent to

[3] For example, in a *normative* sense, see Gerstein (1970) and Parent (1983). Smith (1993) is an example of *descriptive* research aimed at improving *interpretive* understanding. Culnan and Armstrong (2000) and Hann et al. (2002), among many others, serve as examples of *descriptive* research that improves *positivist* understanding. Note that these citations are provided solely as examples and are not intended to represent an exhaustive annotation. For that reason, inclusion/exclusion of a certain article implies nothing about its quality relative to other publications.

privacy research than to any other type and, while it is regrettable when it occurs, the problem is an obvious one. In my view, a large number of Roger's concerns such as alleged misuse of Likert scales or undetected and uncorrected response bias can be attributed to such sloppiness on the part of some researchers.

Second, a more subtle problem can emerge - one that may indeed occur with more frequency in privacy research than in some other areas. A researcher may (perhaps unwittingly) intermingle research approaches from these categories in a single study. When intermingling occurs, the outcome is seldom a positive one. Even if a portion of the study was performed with rigor according to the standards of that research category, it is unlikely that the other portions were performed with equal rigor according to the standards of their own categories. Added to this difficulty is that reviewers and editors are usually confused by these multi-category studies, since they are not always clear about which standards apply. The outcome for such papers is seldom a positive one.

For example, assume that a privacy researcher wishes to proffer a normative privacy argument - for instance, that individuals' medical information is sacrosanct and that the normative duty of IS professionals is to protect it, no matter how much such protection costs. If such a normative argument were well defended under the rules of moral discourse, as established by the discipline of philosophy, the paper might well find a home in a highly ranked journal within that domain. But suppose that, instead, the researcher masks that normative argument by presenting the paper as an interpretive study of hospitals' approaches to medical privacy or as a positivist study of hospital administrators' decision-making regarding privacy issues. Researchers who try such a mixed-category approach sometimes consolidate their normative assertions in the paper's Discussion section, in which case reviewers frequently view them as unfounded since they go far beyond the paper's descriptive findings. Or, even more alarmingly, the researchers simply intersperse their normative assertions

covertly throughout the paper so that the Theory, Methods, Analysis, and Results sections read more as value-laden diatribes than as reports of the research process. Such mixed-category papers will not be accepted by philosophy-based journals, since they do not contain normative arguments that can pass the muster of that discipline's review process. But such papers are also usually rejected by top journals that publish descriptive research, such as *MIS Quarterly* or *Information Systems Research*. The mixed-category papers therefore languish in an unpublished state, scorned by both the normative and descriptive research outlets.

If privacy researchers constrain each of their papers to *one and only one* of the categories (normative, descriptive-interpretive, or descriptive-positivist), and if they then perform their research according to the rigorous standards of that category, their chance at publication in a top outlet is good. Falling below those standards, or mixing categories in a single paper, will seldom lead to success. Thus, although Roger claims that one cannot produce good research on privacy and publish it in top outlets, I disagree.

DUNCAN LANGFORD'S REACTION

While I agree with many of the points Roger makes, in practice I feel it may well be impossible for researchers to actually respond to them. For example, it is certainly true that attitudes to privacy differ, depending upon where in the world you're asking your questions - but what should a researcher actually do about it? In practical terms, the limits of the society within which research is being carried out must inevitably shape and constrain the process; so an informed privacy researcher in Sweden will inevitably take a different approach than someone in the UK, or the US, undertaking apparently similar work. While the problems of privacy research are certainly clearer to me after reading Roger's paper, I confess it engendered feelings of depression at the intractable nature of the effects of global variation on the issues he describes. In the light of these points, if there is to be any commonality of approach in privacy research, what can

possibly be taken as a baseline? A further, and connected, point - who will be interested in the results of such research, given the parochial nature of much privacy perception? Perhaps, as IS privacy researchers, we are of necessity constrained to working within a specific culture or society?

BOB KUO'S REACTION

Can we make progress in privacy research?

Roger's observation concerning the quality of privacy research is excellent. Here I would like to switch the attention to a related and equally critical issue: can we make progress with all these problems confronting (self-claimed) privacy researchers? In attempting to answer this question, I must go back to Thomas Kuhn's [1970] analysis of how science makes progress. According to Kuhn, scientists are engaged in what he calls normal research, which is really mundane, puzzle solving type of work governed by a particular paradigm. But puzzle solving also leads to progress because the scientist community's collective faith in the paradigm allows the knowledge to be accumulated, evaluated, and at the time of crisis, revolted. In a sense, progress is possible because the community agrees on the same measurement prescribed by the paradigm. A crisis is created when this agreed measurement no longer serves the community well (that is, the prediction fails to match the observed data). The crisis then leads to revolution, after which a new paradigm emerges. This path of progress thus consists of three stages: puzzle-solving, crisis, revolution. We may call this the scientific version of creative destruction, which is rather costly but unavoidable if scientific progress is to be made.

In contrast, in pre-paradigm scientific work, individual scientist's work can be rather creative. Yet, without the guide of paradigm, the community is divided and progress cannot be made because no consensus on the measurement and, therefore, on what constitutes the progress.

My view of the current state of IS research in general, and privacy research in particular, is that they are in this pre-paradigm phase where we see a lot of creativity but the entire community suffers because of the division. The problems that Roger articulated in a way is a testimony to my observation. For example, the existence of many different attitudinal measurements reflects the creativity of individual researchers. But these works may not be commensurable with one another and, as a result, progress cannot be easily made from the perspective of the community.

My thinking is that if privacy research is to make progress, scholars must play dumb and become engaged in puzzle-solving type of work. We have to stick to a paradigm, even when we know it is full of all sorts of problems. We have to be laboriously content in solving puzzles before we become creative because only in this way can we exhaust the problems confronting us. Finally we have to be courageous when the time comes for us to destroy the paradigm.

My argument sounds like the old one about the diversity of IS research. But it really is not. I support that the community of IS researchers can study a diversified set of streams. My point is that in order to make progress, the small circle of researchers for each stream must be engaged in normal research, i.e., engaged in puzzle-solving type of mundane work. The small group of researchers must first agree on the paradigm and specify the requirements for selecting observation sites for data collection. (Roger's many comments will be very useful to lay out these requirements). They may employ a standardized set of ethics vignettes as research instruments. Such work is certainly not glorious but it is useful in making visible, though small progress for the community. Inevitably, it also creates crisis, which in turn leads to the creative destruction that the community needs for major advances.

III. H. JEFF SMITH'S POSITION AND PANELIST COMMENTARY

Although some of the issues associated with privacy research are similarly applicable to other domains of inquiry, one set of issues is particularly salient for research directed to privacy-related topics: cross-cultural differences. Indeed, unless researchers are sensitive to these differences, generalization of their work may be problematic.

The cross-cultural differences associated with privacy are particularly pronounced between the U.S. and Europe. Several observers note that, while European countries view privacy as a "human right", in the U.S., it is viewed more as a matter for contractual negotiation. Differences are substantial, particularly with respect to regulation.

Based on Bennett's [1992] work, we can categorize countries' approaches to privacy regulation in one or more of the following five categories (an example of each is provided)[4]:

1. The *Self-Help* model, observed in the U.S., depends on data subjects' challenging practices they find to be inappropriate. They are expected to identify problems and bring them to the courts for resolution.
2. The *Voluntary Control* model, also seen in the U.S., relies on corporate self-regulation. Each organization is expected to monitor its own compliance through a mechanism of its choosing (e.g., internal ombudsperson).
3. The *Data Commissioner* model, used by Germany, creates a separate governmental entity that acts as an ombudsperson. To that end, the commissioner receives and solicits complaints from citizens and performs investigations. In addition, the commissioner offers advice to firms and other organizations regarding data handling, makes

[4] This discussion draws heavily on Smith [2001].

proposals to legislators, and may inspect some organizations' data processing operations.

4. The *Registration* model, embraced by the U.K., requires that each organization maintaining a databank containing personal data registers (usually upon payment of a fee) that databank with a separate governmental institution (usually called the "Registrar"). The Registrar can "deregister" a system based on a complaint and investigation.
5. The *Licensing* model, employed by Sweden, requires that each organization maintaining a databank containing personal data secure a license for the databank (usually, upon payment of a fee) by a separate governmental institution (in Sweden, this institution is known as the Data Inspectorate). This institution is also responsible for establishing specific conditions for the collection, storage, and use of personal data. This model requires *prior* approval by the regulatory institution for any use of data.

Note that no governmental "bureau of privacy" or similar agency takes overall responsibility for privacy regulation under the Self-Help and Voluntary Control models. However, such an agency is necessary under the other three models. For example, the EU demands that each member state provide a centralized privacy agency of some sort.

In addition to the regulatory structures, we can further distinguish the U.S. and many other countries based on the extensiveness of a data subjects' rights. With a few exceptions (for example, credit reports), U.S. law does not reuire that data subjects be allowed to inspect their own records and make corrections to them. Yet the right to access one's own records and challenge their accuracy is a fundamental precept of European law, and this right extends across all sectors and across almost all data types.

In addition to provisions for inspection and correction, secondary uses of data receive different treatment in the U.S. and Europe. For the most part, federal U.S. law seldom requires that data subjects be told about secondary uses of data (that is, when personal data are collected for one purpose but used for another) or that the data subjects be given the right to stop those uses. However, some firms in many industries disclose such uses, and some have also provide "opt out" capabilities for data subjects. (Under such plans, unless the data subject takes overt action to "opt out" of the secondary data uses, it is assumed that the data subject assents to the use). Sometimes, the firms do this voluntarily, but on other occasions pressure is applied by either legislative bodies (e.g., Congressional subcommittees) or other legal entities (e.g., state attorneys general).

But, with very few exceptions, secondary uses of personal data in Europe are prohibited if the data subject objects to the secondary use. Usually, a clear and overt notification of the intended uses is given at the time of data collection, and the data subject is provided an easy option (often a check-off box) to object to the secondary use. If an organization later realizes it wishes to use the collected data for a new purpose, it is obliged to contact the data subjects and allow them to object. While the precise nature of these contacts and the form of the objections varies across countries, the notification must always be clear and overt, and the objection procedure cannot place much of a burden on the data subject.

Beyond these protections, though, some European countries demand that an "opt in" approach be embraced for all secondary uses, and an "opt in" provision must be used in any European Union (EU) country if the profiles include special categories of data (e.g., racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, or sex life). Under an "opt in" plan, an organization cannot assume that the lack of an objection implies

consent. Quite the opposite, data elements can be used only when the data subject gives his or her overt permission.

Thus, countries exhibit significant differences in approaches to privacy regulation and in the rights accorded to data subjects. While the above discussion focused on the differences between the U.S. and Europe, it should be noted that many other developed countries, such as Australia and Canada, also embrace structures that are consistent with some of those seen in Europe [see Milberg et al., 2000]. To some degree, among developed countries, the U.S. structure should be seen as more as an outlier than as a mainstream approach.

The error that can be made by privacy researchers, of course, is to conduct a study that is grounded in one or two countries and - without qualification - to claim that the findings are applicable in many other locales. It is human nature for each of us to assume that others in the world share our cultural values and approaches. However, in the domain of privacy, there appear to be few conclusions that one can draw - at least in a descriptive sense - that apply around the world. In other words, a study of privacy attitudes, policies, or practices that is conducted in the U.S. will not usually be that informative to a manager in Sweden. While there is nothing wrong with researchers doing work in their own locales (and, indeed, I have done my share of that!), we make a big mistake if we do not bound our conclusions appropriately when we report them.

ROGER CLARKE'S REACTION

I concur with Jeff's main point, that the meaning of privacy is culturally-dependent. However I find several problems with his argument.

1. He uses the term 'cross-cultural differences' but then talks exclusively about nation-states. Privacy protections must also be sensitive to cultural differences within jurisdictions. Ethnic, lingual and religious aspects of culture are critical. That applies as much to the differences between, say, the U.S.'s 'Bible Belt' and permissive downtown San Francisco; and between Hispanic and 'Native

American' people; as it does to, for example, East Asian Confucian values compared with northern European 'open society' ideas.

2. Bennett's [1992] list of categories misses an important model intermediate between Voluntary Control (2) and Data Commissioner (3). Co-regulation blends legislation with codes specific to particular industry sectors and particular practices. The New Zealand legislation of 1993 is commonly put forward as an example [Clarke 1999].

3. It would be easy to infer from Jeff's description that the U.S. is a 'privacy law free zone'. Nothing could be further from the truth. Well over 200 U.S. statutes directly address privacy. They fill large books, such as Smith [2002]. The U.S. legislatures steadfastly refuse to enact generic privacy protections into law. As a result, there are continual explosions of public disgust at one or other gross abuse of privacy by government or business, which culminates in knee-jerk, highly specific legislation. The rest of the world considers it to be an indicator of a pathological condition that the most highly-protected data in the U.S.A. are the contents of video-rental records (as a result of disclosures of the viewing habits of a person proposed for appointment to the U.S. Supreme Court).

Finally, Jeff is correct in saying that the U.S. seeks to deny that privacy is a human right. But that's indicative of flagrant disregard by the U.S. of its international undertakings. A couple of inconvenient international instruments (called the Universal Declaration of Human Rights [UDHR 1948] at Article 12, and the International Covenant on Civil and Political Rights [ICCPR 1966] at Article 17) make clear that privacy is a "human right" (with or without the quotation marks that make it look like some term unrecognised by the law and used only by dreamy socialists).

DUNCAN LANGFORD'S REACTION

I'm with Roger in his perception of the US as having a somewhat bizarre take on privacy; however, such an approach is inevitably consequent upon the American legacy of a patchwork of special-case legislation, rather than the European approach which follows a more centrally defined legal concept of privacy. Of course, given the political will, the inclusion of human rights within the US would surely be possible; but recent events show all too clearly the improbability of a strong central authority allowing potential – or actual - privacy risks to its citizens to place even the slightest constraint on its actions.

BOB KUO'S REACTION

On the cultural and regulatory differences, my experience in America (17 years) and in Taiwan (30 years) tells me that actually the word privacy means very different things in these two countries. In Taiwan the first time the word privacy appeared in regulation was only about four years ago. Still, I suspect that deep differences also exist between Taiwan and the U.S. as well as between the U.S. and other countries. Jeff already pointed out the differences in regulatory structures across countries, which reflect more or less the differences in cultural conceptions of privacy. Note that the difference exists not only in privacy but also in other rights, such as intellectual property rights and freedom of speech. Yet, the trend of globalization brought forth demands to change local conceptions of these various rights. Some regulatory changes were made, like the one in Taiwan. But these changes may actually be counterproductive in the short term. For example, some lawsuits were brought to the court after the passage of the privacy law in Taiwan, but their verdicts seem to confirm to the traditional conception of privacy[5]. These lawsuits certainly do not help in ensuring privacy as a universal right for all. The same also happens in the area of intellectual property rights, in which the many prosecutions led to the complaints that the copyright laws only serve the rich and powerful rather than to encourage

[5] The traditional way in Taiwan says that the more powerful people have more privacy rights than the less powerful ones, and that the more powerful agency has the right to violate the less powerful ones' privacy. In addition, the traditional sense of privacy has more to do with utility than with a certain set of values/virtues.

creativity for ordinary citizens. The same types of complaints exist in the US as well [cf. Lessig, 1999].

It is already difficult enough to study privacy in different contexts. Now, the context seems to be moving. This shift certainly heightens the challenges to researchers who are studying privacy in cross cultural settings. I agree with Jeff that researchers must be careful in drawing conclusions on their specific research work. I also think that it may be useful to generate a test bank of privacy scenarios for use by researchers across cultures. The use of standardized test materials and the employment of the commonly accepted measurements allow the community to compare and contrast their research results. Differences between cultures may also be revealed systematically. This approach is essentially the normal research I suggested earlier in responding to Roger. While this approach is no panacea, the accumulated insight over the long term will be great.

IV. DUNCAN LANGFORD'S POSITION AND PANELIST COMMENTARY

The central topic of Information Privacy may be approached by IS researchers from a number of different directions; several, of course, are addressed in this paper. While the privacy aspects of IS work within organisations may perhaps be less frequently considered than other features of privacy research, they are nevertheless an issue worthy of serious attention.

Consideration of this area is particularly relevant because virtually all IS research is probably carried out from within an organisation, whether it be academic or commercial. However, despite an organisational base, research assumptions normally tend to be made without specific awareness or consideration of organisational influences. While privacy issues can obviously arise directly (e.g. in workplace surveys and/or response bias arising from insufficiently credible assurances of confidentiality) to ensure appropriate privacy of information, the

less noticeable influences of the containing (or instructing) organisation itself may need to be considered specifically.

One of the most significant aspects of organisational influences is almost certainly their invisibility. Simply because organisational influences are automatically accepted as a normal part of working within a particular institution, such influences are understandably seldom identified and specifically related to individual IS research. Unless expressly sought and identified, they may therefore simply disappear into the background.

Unfortunately, due to immense variations in organisational structures and philosophies, the categorisation of organisational influences is by no means straightforward. For simplicity, and the limited purposes of this analysis, it may be considered that such influences would normally fall into two distinct groups – overt and covert.

Overt

Overt influences describe specific company rules or policies, dictated and enforced directly by management. Such policies will naturally reflect an approach – for example, to data collection and distribution – officially considered appropriate by that institution. While it might be felt by an outside observer that all researchers within a particular organisation would automatically be aware of such formal policies, this can by no means be assumed. It is perhaps unusual for an IS researcher to spend very much time in clarifying the globally prescribed procedures of their employer, however logical it might seem for them to do so.

Covert

Possibly of rather greater concern to an IS researcher than an organisation's formal policies, however, might be *covert* influences – oblique or hidden pressures to conform or behave in a way locally viewed as acceptable. Covert

influences within an organisation may come not only from managers at all levels, but even from colleagues. The effects of covert influences are likely to be both subtle and various, and will obviously take their shape from the containing organisation. Examples include the unwritten expectation that, whenever requested, personal data will be automatically shared with other researchers; that oversight of confidential material by researchers and others unconnected with the project is appropriate, and so on. Expectations that management might request sight of confidential material, for instance raw personal data, may well be more formalised, but examples certainly exist of commercial pressures dictating the unceremonious breaking of IS research security.

Perceptions

An associated issue concerns the question of *perceptions*; history is familiar with examples where what is individually acceptable becomes less so when public perceptions allow the consolidation of material. An historical example lies with Census demographics, which once used the number of windows as a measure of affluence. While this information was publicly available, individuals understandably became upset when the government collected and used this data. When we relate the perceptions of colleagues and data subjects to the methodologies of IS research, it is clear that information privacy issues may potentially arise. For example, regardless of the real situation, IS research carried out by academics representing a university may well be publicly perceived as taking a more responsible attitude to the security of collected data than similar research undertaken by a private commercial organisation, with resultant effects on the attitudes and cooperation of data subjects.

In contemplating the particular information privacy issues inherent in IS work within an organisation, we have now considered two main areas of possible concern, and a third associated concern. Specifically, these are the risks of privacy being at risk through specific rules and policies introduced directly by management; by informal pressures or assumptions brought about by workplace

colleagues; and by a wider awareness, perhaps of analysis taking place based upon previously available (but previously unanalysed) data.

Data Reuse

To these central issues may be added a final IS hazard associated with large organisations – that of data, once having been collected for one purpose within the company, being later made available for other, unrelated, purposes. What in its original form might well be data of limited personal risk might, if later combined with additional material, allow individuals to become far more vulnerable; and of course in today's multi-national business world, the movement of data globally is no longer unusual. Even while possession of IS research data might still technically remain within a single organisation, a shared view on the appropriate use and security of that information can no longer be assumed.

Conclusion

In this section I identified a number of issues specifically related to the risks for information privacy within organisations. I emphasised the importance for IS researchers in making themselves aware of specific policies established by their employers relating to their work, and stressed the necessity of also becoming aware of less formal pressures on information privacy, which I labelled covert influences. The relevance to IS research of public perceptions of an organisation was also mentioned. Finally, some possible risks to information privacy when IS research is carried out from within a multi-national organisation were described .

Of course, organisational influences may create possible threats to information privacy in many orther areas. In the space available, this section could do no more than briefly discuss a few of these areas, in the hope of sensitising researchers - and others - to some potential risks.

ROGER CLARKE'S REACTION

Duncan observes that "virtually all IS research is probably carried out from within an organisation". That was tenable several decades ago, but long since ceased to be a sufficient scope-definition for IS research. Inter-Organisational Systems

(IOS) have been much-discussed since at least Malone et al. [1987]. Clarke [1992] introduced the term 'Extra-Organisational Systems' to refer to the very different category of systems in which individuals and unincorporated enterprises are significant players.

A study of workplace privacy can reasonably limit its scope to intra-organisational factors; but most privacy research cannot limit itself in such a way. The values that provide the reference-point for discussion are external to the organisation. So are the laws. So are the people whose privacy is being discussed. I argued earlier that the performance of quality research in domains in which privacy is a significant factor is extremely difficult. The need to move beyond the comfortable environs of a single organisation is one of the challenges.

BOB KUO'S REACTION

Let me first introduce a study [Lin, 2003] conducted to investigate the impact of organizational policies on employees' self-regulatory competence in sanctioning themselves against privacy invasion. The study was conducted because today, many privacy abuses can be traced to the lack of organization policies governing the conduct of the personnel who are in charge of managing the information systems. IT professionals, who are the most important gatekeepers to the information privacy practices, carry the oversight responsibility for information privacy since their knowledge of their organization's systems and data is most extensive. Previous research suggested that at the organizational level, managerial policies concerning ethical codes and rewards/penalty perception may influence IT professionals' self-regulation capacity against privacy abuses. The self-regulation capacity is indexed by IT professionals' ethical judgment, subjective norm, privacy self-efficacy and intention, which, according to the paradigm of self-regulation, may reciprocally interact with the organizational use of ethical codes and rewards/penalty system.

Thus, we first proposed an ethical decision model based on the paradigm of self-regulation and validated the appropriateness of this model for studying information privacy. We then demonstrated how the perception of ethical codes and the rewards/penalty may impact the ethical judgment, subjective norm, privacy self-efficacy, and ethical intention. We found that the rewards/penalty perception moderated the relationship between ethical judgment and intention, and that the ethical codes moderated the relationship between privacy self-efficacy and intention.

During the period of the study, many problems that Duncan raised were encountered. Nevertheless, we believed that a well designed study that concentrated on a few key variables could still reveal important insights. At the end, we believed we did have this insight. Specifically, we found that while the individual level of competence in sanctioning against privacy abuses did not fluctuate with organizational policies concerning ethical codes and penalty/reward treatment, the exercise of personal control did fluctuate. Simply put, in morality, while people's perception of self-competence does not fluctuate with the situational changes, their way of executing this self-competence does change. We believed that this finding was important in ethical research, which was criticized for overlooking the knowing-acting gap in ethics (that is, people are knowledgeable of ethical requirements and intend to be moral, but their actions vary according to the situation).

This experience shows that organizational issues for privacy research can be studied. Of course, the problems raised by Duncan and earlier by Roger all exist. But a rigorous study does not mean it is problem free. Thomas Kuhn's analysis of scientific progress tells us that virtually all scientific studies carry their own set of problems over which researchers themselves do not have control. But progress can still be made if researchers are willing to be engaged in normal research.

V. BOB KUO'S POSITION AND PANELIST COMMENTARY

THE ABSURDITY OF PRIVACY INFORMATION TRANSACTION

In the 2002 ICIS conference, papers on "motivating consumers to disclose personal information" [Tam et al., 2002] and "measuring the cost-benefit trade-off" [Hann et al., 2002] were presented. I am personally concerned about the blindness behind this line of research. The so-called privacy information is about "what I am". But in the following, I am going to argue that "what I am" is really socially situated. The information loses its meaning once it is separated from the situation in which it is used. My argument is based on the work of Goffman [1959, 1961, 1963, 1967] on the presentation of self (i.e., the presentation of "what I am").

But let me give some examples related to "what I am." In Taiwan, there is very popular bulletin board system (BBS) called PTT, used primarily by college students. Tens of thousands of them spend hours every night surfing PTT. Here, if you want to find some particular individual, say, a pretty girl, who has left her purse in a train station, you do not need to provide much identification information. There is no need for name, age, major, address, etc., just the name of the college and when/where you saw this girl. Hundreds of students would find her for you, in a matter of hours or even minutes. In this case, "what I am" is not defined by attributes like name, age, major, address, etc., but is embedded in the social network of college students in PTT. Likewise, if a student complained of an injustice, say, he received a grade of D from an "old, stubborn, male" professor, the social network of PTT students might identify this professor fairly quickly. Note that in this case, not only is "what I am" socially embedded, the "perceived injustice" has to be present to trigger PTT surfers to conduct the search for "what this professor is." In other words, if someone posted a request to find an "old, stubborn, male" professor, probably very few PTT surfers would bother to do the same. In fact, more specific information like college and

department can be provided, but few people might be interested in knowing "what this professor is." Indeed, there appear to be several typical "scripts" in PTT: it could be a "helping someone" script or a "fighting some injustice" script. The same information would have very different meanings in different scripts, and the consequences for identifying "what I am" would be very different. "What I am" is therefore socially situated, and the information loses its meaning once it is separated from the situation in which it is used.

A theory that can help us to understand the above examples is the self-presentation theory by Erving Goffman, whose study of self leads to the theorization that self, i.e., "what I am," is constantly changing, depending upon how one perceives the events with which he or she is confronted with. Goffman's theory is difficult for me to put in words. Fortunately, I have used the book, The Forest and the Trees: Sociology as Life, Practice, and Promise by Allan Johnson (1997) as the text in a course I have taught. It has helped me to understand Goffman's work greatly and I am forever in debt to Professor Johnson for my thoughts as expressed in the following material.

According to Goffman, people's roles and statuses are the legacies of social designs by the society in which they live. For example, the statement "Bob is a 47 year old male professor and father of two" contains so-called privacy information. But all the labels (i.e., Bob, 47 year old, male, professor, and father) are products of a certain culture and each label carries a set of expectations that are determined by the culture, although these expectations vary across cultures. More important, the specific use of the labels and their specific expectations vary even across situations. For example, the statement "Bob is a 47 year old male professor and father of two" has a particular meaning in Taiwan that is different from that in the U.S. or Nigeria. More specifically, the same statement means different things when it is mentioned in an "injustice PTT script" or in a "classroom script." Given that the meaning of this information is socially situated,

I as an individual do not really have much to say about the various uses (meanings) of the different labels that describe “what I am.”

The labels are constraining in nature: they represent the set of behaviours that I must conduct to match the typical expectations of that particular label designated onto me by the society. Sometimes the revelation of these labels can be harmful to the individual who may not control the consequences of wearing these labels. Why is there then such a rush to trade these labels, or so-called privacy information?

PRESENTATION OF SELF: THE SOCIALIZED WAY OF BEING

Furthermore, in the view of Erving Goffman, people are social beings who wish to be accepted by other people and, thus, are constantly engaged in practices to avoid being embarrassed or embarrassing others. To do so, one must pay attention to differences in various situations so that he or she can act properly. How may any individual master the skills needed to handle different situations? Goffman’s study of people’s social interactions led him to his famous dramaturgical analysis. In short, Goffman sees an individual’s social encounters in daily life as resembling a journey composed of a collection of plays that take place in streets, schools, offices, and places like restaurants or parks. These plays are legacies of cultures, and cannot be made entirely explicit. It is very difficult to pinpoint when, where, and by whom a play is written. Plays have actors as well as audiences, and each individual in the play is an actor being watched by one or more audiences, but at the same time is also an audience watching others' plays. Early in their life, people of a specific culture would learn what a typical play should be like as well as the typical rules and routines for each role of that play. This allows them, in social encounters, to imagine a particular play, either consciously or unconsciously, as well as how to perform a particular role properly during a play. In Goffman’s view, it is critically important for individuals participating in any play to keep that play coherent, i.e., to keep the play going as expected. The goal of an individual, therefore, is to be

recognized/received as a good team member of the play so that other actors and audiences can maintain positive images of him or her. In a traditional society like Taiwan the plays in work or school may have rather strict scripts that people must follow, while in a more liberal society like America, people are allowed to be more flexible. Still, many other plays are unplanned, i.e., a teacher may fall unexpectedly in the classroom and, when it happens, both the teacher and students would have to improvise to resolve the embarrassing situation. Thus, in social life one cannot cease to act, and the type of acting is dependent upon the cultural scripts and the role that the actor assumes.

Consider, for example, that the 47 year old professor takes his family to have dinner in a restaurant. During the dinner, the young children become unsettled and start fighting. If this happens in Taiwan, the mother might punish the children, probably not because she is agitated by the children's behavior but because for Taiwanese, a "responsible" mother is supposed to discipline her children, which would earn her the respect of the audience (other guests in the restaurant). Afterwards, the professor would probably give the children a lecture in how to maintain good manners, not because he is an expert on manners but because doing so fits the role of a "responsible" father and probably also the role of a "professor." However, if this incident happened in a restaurant in America, a very different play would be acted out by the parents. In fact, many restaurants anticipate young children's energetic behaviors and set aside a playground for children, who would then be encouraged to explore and have fun. In doing so, parents can enjoy their time having a quiet dinner, while other guests may not even notice children' adventurous behaviors unless they happen to be near the playground.

There is a good reason that I use restaurant as the example: since my return to Taiwan my wife and I have been called "irresponsible" many times because we act like we were back in America. Since we neither wanted to discipline the children nor to disappoint the audiences, my wife and I had to improvise to satisfy

audiences when this happened. And, as one might expect, we failed quite often. At that time, sympathetic audience would pretend nothing has happened, but some not-so-friendly audience would give us a bad look. Worse yet, in our culture, failure in a play may even carry the price of stigma. As a result, my wife became so frustrated that she sometimes refused to take children to a restaurant until they were older and learned how to behave like normal Taiwanese youths. Note that it is not just restaurants, but also schools, hospitals, etc. so that we have "earned" ourselves many not-so-desirable descriptions, which, from the privacy perspective, have serious consequences for our life, like small social circles. I have learned that it is virtually hopeless to try to explain to others why we did what we did (not to discipline the children): the culture dictates what constitutes a good play, a good script, and what are good/right and bad/wrong performances. If I wish to be approved by people around me, I have to accept the roles and properly enact these roles. Just as Goffman suggested, I am like an actor on a stage that can hold many different plays. I may use different techniques – wearing proper make-up and clothes that I believe can best fit the occasion, choose labels that I believe can best depict my status and roles for that occasion - to make my performances appear to be authentic. Yet, the existence of one authentic self seems to be unlikely as I assume the various roles role in different plays and do my best to turn in my performances that may inevitably conceal/conflict my real self (Johnson, 1997). That is, when the journey is over at the end of the day, the various "what I am" from various social encounters may not collectively add up to a coherent image of myself. So if someone has heard what happened about me in an event and asks me to authenticate it, I would probably respond with "Well … it is not like … the situation was … So I did … , but I did not mean to …" Actually, it's easy to question if anyone has an authentic social self at all when we view social life as theatre. No wonder that the author, Allan Johnson, would conclude that "Whatever that performance, it comes from somewhere in me, and if there is an unreality in it, it's in my not being aware of that simple fact and denying my connection to the consequences

my behavior produces. As such, the problem of authenticity isn't that we're performing or managing impressions. The problem is that we don't embrace and own our actions for what they are as part of who we are. The problem isn't that we have so many roles to perform that can make us appear inconsistent or other than we'd like. The problem is that we don't integrate them with an ongoing awareness of the incredible complexity of ourselves and the social life we participate in" (Johnson, 1997, pp. 153-154).

Note that in Goffman's theorization of self, there is the concept of backstage where one can have private life. But this concept is rather irrelevant in the Internet since virtually everywhere in the Internet may become public, as demonstrated in the previous examples of PTT. Often people socialize with others in the Internet without knowing about who and what a particular person really is. What is known consists primarily of cultural images of the "typical" person - the typical professor, the typical student, etc. In interacting with others in PTT, people are keenly aware of that they are watched by others and, subsequently, carefully enact the routines that allow them to be received positively. In addition, in various social interactions within PTT, as those in many other parts of the Internet, language is the primary medium employed to enact the plays. Since language always involves implicit cultural beliefs and assumptions that cannot all be made explicit, in the Internet environment we are who people think we are, a reality of us they construct from cultural ideas.

CAN PRIVACY BE TRANSACTED?

The previous essay centres around the concept that self is fundamentally a social concept that describes the way of being. According to Johnson (1997):

1. We create impressions of "what I am," what Goffman called "the presentation of self," based on plays that we learn, knowingly or unknowingly, as a member of a culture.

2. People's knowledge of what a person is ("what I am") does not have to be based on direct experience. Rather, this knowledge may be based on the cultural beliefs associated with the roles and statuses of that person who, in social interactions, would likely perform the cultural routines that fit these roles and status so as to avoid embarrassment or embarrassing others.
3. Thus, the line between what a person is and how he or she may participate in social life isn't as clear and neat as that interpretation makes it seem. One must negotiate with him or herself in bridging the gap between the observed reality and cultural interpretation. This negotiation is not straightforward.
4. As a result, one's relationship to a system's culture is both dynamic and alive, with the person creating the world as much as he or she is created by and through it.

In fact, one would quickly run out of terms in attempting to provide labels that can define the relationship between people and systems, Thus, the labels that describe "what I am", i.e., the so-called privacy information, is not objective, as many information technology experts like to believe. Rather, it always includes implicit beliefs and assumptions that cannot all be made explicit. In our daily life, practical, cultural understanding of these labels is more fundamental than its detached, objective definition. Furthermore, these labels are constraining in nature. It is virtually impossible for any individual to invent a new label to describe who s/he is. At best, s/he is allowed to choose one that can serve him or herself well (e.g., Bob may work hard to become a professor). At worst, and probably more often than not, the labels are designated onto the individual without his or her consent (e.g., 47 year old, male, strict, dull). Note that the culture does not simply designate a label onto a person. It also dumps a whole set of behavioural expectations that limit what this person must do. Violations of these expectations can be harmful, depending upon the situations. And yet, what constitute

violations could be entirely out of the control of the individual. Thus, how can I trade in this privacy information that is fundamentally social and that I am unwilling to fully authenticate? How, then, can we "objectively" design a transaction system for privacy information? The foregoing does not mean that we can deny that companies are attempting to purchase the privacy information and that some people would trade their "who I am" labels for some financial gains. But, in view of the aforementioned arguments based on Goffman's work, is it really possible to measure the cost and benefit of privacy information transactions?

ROGER CLARKE'S REACTION

By asking 'can privacy be transacted?', Bob accepts without demur the peculiarly American attempt to avoid privacy as the human right that it is in international law, and in most national laws (including America's). Reduction to a mere 'economic right' would be repugnant to the notion of humanity [Clarke 2000, section 2.5].

Note that I do not not deny that there is an economic dimension to some aspects of privacy. Individuals can provide consent to the collection, use, and/or disclosure of data about them (possibly informed consent, possibly freely-given consent, and hence possibly meaningful consent), in return for some consideration. That privacy advocates are continually startled by how little most individuals accept as consideration cannot alter the idea that some human rights include the freedom to trade the right against other interests. This is, of course, not the case with all human rights: a person is not permitted to sell themselves into slavery.

It might also be feasible to impute an economic value for privacy *ex post facto*. That analysis is no different from the way in which we can compute the value of human life by calculating the cost to put all electricity supply underground, and

dividing that by the number of people who die in collisions with lamp-posts. But that produces an implicit valuation. It is not a 'price tag' for privacy.

The U.S. devaluation of privacy seeks to go much further, however, by denying that it is a human right at all. Corporations face the risk that too many people may charge too high a price; or they might even exercise their nominal right to charge an impossibly high price; or worst of all, they could refuse to bargain away what they correctly consider to be a human right. In that case, the U.S. position would clearly be that the balance of the economic right would need to be shifted in favour of corporations, to ensure that marketing costs remained low.

Finally, note that the 'economic right' notion makes even less sense in the context of the use of personal data by governments, because parliaments override privacy rights outright, rather than qualifying them.

Researchers (at least those working within the scientific tradition) strongly desire to express concepts as quantities, and preferably as financial values. Because privacy is a human and not a mere economic right, the reduction of privacy to quantitative measures is fraught with danger. The cultural dependency of privacy and the supra-organisational scope of the research domain, discussed earlier in this paper, compound the challenges confronting the researcher.

DUNCAN LANGFORD'S REACTION

Examination of a trade in privacy information will undoubtedly produce different results when considered from differing global perspectives. Of course, in this field many researchers and writers are from the United States, so one essential point of difference is a depressingly common sociocentric perception which assumes the U.S. condition to be natural and normal, when from a global perspective it is in fact far from either. Of course, in a full-blooded capitalist state, *everything* can be given a cash price; why therefore should privacy claim any rights of

exclusion? I believe privacy is a human right, as is freedom; but, just as slavery may be justified on purely economic terms, so may restrictions on privacy.

VI. WHERE NEXT? ROBERT DAVISON'S CLOSING REMARKS

The position statements of the four panelists in this paper go far beyond what was presented or discussed at ICIS in Barcelona ten months ago. They are the accumulation of an extended series of email conversations between the panelists and the panel chair. While all four contributions focus on privacy in one or other of its many forms, the four positions here are not neatly juxtaposed to each other. Indeed, as Roger wryly commented a few weeks ago, not only was the process of getting positions and commentaries akin to the herding of cats (more like Bengal tigers without dinner for a week), but further attempts to engage in a reasonably coherent discussion or integration of the four sets of positions and associated commentaries would be difficult in the extreme.

Consequently, rather than attempt that integration, I propose instead to draw upon these various perspectives in a separate, short tail-piece of my own. I share with Roger deep concerns about the way privacy research is subject to innumerable influences quite beyond the researcher's control (including those related to publication, to public and government perceptions of privacy, to methods appropriate to the research of privacy issues) yet nevertheless highly relevant for the transferability and publishability of that research. Yet I share Duncan's unease about the implications of these differences and influences – where is the base line? Is there any point in privacy research if it is to be so highly contextualised that any results will only be of interest to a small minority of readers? Perhaps the counter argument to that is that when (God forbid) we become a single world culture, then we will all share the same context! This line of argument does not seem very profitable, but it usefully raises the issue of parochialism: are readers of privacy research only interested in what is relevant to their own context? The same question is asked in other disciplines. A decade

ago, Boyacigiller and Adler [1991] noted the parochial dinosaur that research into organization science had become. In a recent special issue of the Journal of Business Research, Peng et al. [2001] emphasise the need for China-focused business research to be integrated into the mainstream, with researchers making larger theoretical and methodological contributions. Why should not the same be true of research into information privacy? Indeed, this question is precisely the one that Jeff appears to be asking at the start of his commentary on Roger's position. Why should not information privacy research, conducted from an Information Systems perspective, be able to inform other disciplines?

Jeff's own position is one that favours a cross-cultural perspective on information privacy research, though as he correctly in my view points out, any generalisation of findings must be expressed with extreme care. Individual human beings may fondly imagine that their way of thinking is the same as everyone else's, but of course nothing could be further from the truth. Information systems researchers must take particular pains to avoid this error simply because it was perpetrated so many times in the past. The IS literature is replete with accounts of research studies developed and tested in Anglo-American contexts, but whose findings are blithely assumed to be valid throughout the world with little or no modification.

Duncan suggests that much privacy-related research is undertaken within an organisational context, and that the pressures or influences (whether overt or covert) that can be brought to bear within organisations bear further investigation. Cultural influences within the organisational space are interesting in several ways.

1. Any discussion of organisational culture needs to involve some specifics of precisely what we mean by the word organisation: academic, government, private, or just a colloquium of individuals.
2. In our web-centric world, we more and more frequently encounter examples of virtual organisations that operate primarily on the Internet and hence cross

physical borders, most notably those associated with nation states or other forms of sovereignty and jurisdictions. Indeed, the authors of this paper form such a virtual colloquium, meeting face-to-face just once – in Barcelona. Such border-crossing entities may develop their own organisational cultures, but these cultures will be intertwined with the various national and subnational cultures that they encounter in their employees, their customers, and the work practices that occur in different parts of the web space. It seems that virtual organisational spaces offer a fascinating opportunity for research into information privacy.

Bob's sociolinguistic approach to the privacy issues associated with labels and stereotypes is entirely different from that of Roger, Jeff and Duncan, yet it too is cultural in nature: borrowing from Schneider and Barsoux [1997], the same label can result in different meanings, and different labels can result in the same meaning. Given human propensity for stereotyping, and labelling is but a form of this behaviour, a sociocultural deconstruction of labels in use in organisations could provide for some intriguing insights into the way organisations are managed, as well as valuable lessons for cross-cultural and international management.

Where next? Culturally sensitive approaches to the study of information privacy offer much to researchers and practitioners. Many questions are unanswered, particularly in the cross-cultural domain, some of which are alluded to above. Much can be learned in the context of IS and Management practice: culture is a recurring theme at many mainstream conferences, but, as Roger indicates, privacy is not. Privacy is nevertheless a concept that is familiar to an increasing number of stakeholders - be they researchers who must gain ethics committee approval, managers who monitor emails and Internet communications, governments who write legislation, or ordinary citizens and consumers, who are usually the uncared for victims but necessary data subjects. Stakeholder perspectives on information privacy, particularly cross-cultural perspectives,

would be of significant value to an improved understanding and appreciation of the complexities of our society.

Editor's Note: This article was received on August 20, 2003 and was published on October ____. It is based on a panel held at the International Conference on Information Systems in Barcelona, Spain in December 2002.

REFERENCES AND BIBLIOGRAPHY

EDITOR'S NOTE: The following reference list contains the address of World Wide Web pages. Readers who have the ability to access the Web directly from their computer or are reading the paper on the Web, can gain direct access to these references. Readers are warned, however, that

1. these links existed as of the date of publication but are not guaranteed to be working thereafter.
2. the contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. the authors of the Web pages, not CAIS, are responsible for the accuracy of their content.
4. the authors of this article, not CAIS, are responsible for the accuracy of the URL and version information.

Azmi, I.M. (2002) "E-Commerce and Privacy Issues: An Analysis of the Personal Data Protection Bill", *International Review of Law, Computers and Technology*, (16)3, pp. 317-330.

Bandura, A. (1991) "Social Cognitive Theory of Self-Regulation", *Organizational Behavior and Human Decision Processes*, (50)2, pp. 248-287.

Baskerville, R.L. and M.D. Myers (2002) "Information Systems as a Reference Discipline", *MIS Quarterly*, (26)1, pp. 1-14.

Bennett, C.J. (1992) *Regulating Privacy*. Cornell University Press: Ithaca, NY.

Boyacigiller, N.A. and N.J. Adler (1991) The Parochial Dinosaur: Organization Science in a Global Context, *Academy of Management Review*, (16)2, pp. 262-290.

Brendon, C.F. (2002) In Ecommerce, Consumer Trust is no Longer an Option: It is the Requirement for Success, *Proceedings of the Annual Quality Congress*, Milwaukee, pp. 355-361.

Clarke R. (1988) "Economic, Legal and Social Implications of Information Technology", *MIS Quarterly*, (12)4, pp. 517-9, http://www.anu.edu.au/people/Roger.Clarke/DV/ELSIC.html

Clarke R. (1992) "Extra-Organisational Systems: A Challenge to the Software Engineering Paradigm" Proceedings of the IFIP World Congress, Madrid, September at http://www.anu.edu.au/people/Roger.Clarke/SOS/PaperExtraOrgSys.html

Clarke R. (1994) "Human Identification in Information Systems: Management Challenges and Public Policy Issues", *Information Technology & People*, (7)4, pp. 6-37. http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html

Clarke R. (1997) "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", at http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html#Priv

Clarke R. (1999) "Internet Privacy Concerns Confirm the Case for Intervention", *Communications of the ACM*, (42)2, pp. 60-67, at http://www.anu.edu.au/people/Roger.Clarke/DV/CACM99.html

Clarke R. (2000) "Beyond the OECD Guidelines: Privacy Protection for the 21st Century", http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html#Rts

Clarke R. (2001) "Research Challenges in Emergent e-Health Technologies", http://www.anu.edu.au/people/Roger.Clarke/EC/eHlthRes.html

Clarke, R. (2002) "Privacy Laws" http://www.anu.edu.au/people/Roger.Clarke/DV/PrivacyLaws.html

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

Davison, R.M. (2000) Professional Ethics in Information Systems: A Personal Perspective, *Communications of the AIS*, (3)8, pp. 1-33.

Davison, R.M. and N.F. Kock (2002) Professional Ethics, http://www.is.cityu.edu.hk/Research/Resources/isworld/ethics/index.htm

Davison, R.M., R. Clarke, B.F.Y. Kuo, D. Langford and H.J. Smith (2002) "Information Privacy in a Globally Networked Society: Implications for IS Research", Panel Session at the *23rd International Conference on Information Systems*, Barcelona, 915-918.

Davison, R.M., N.F. Kock, K.D. Loch and R. Clarke (2001) "Research Ethics in Information Systems: Would a Code of Practice Help?", *Communications of the AIS*, (7)4, pp. 1-39.

Fluendy, S. (2000) "Personal Values", *Far Eastern Economic Review*, (160)4, p. 26.

Gerstein, R.S. (1970) "Privacy and Self-Incrimination", *Ethics*, (80)2, pp. 87-101.

Goffman, E. (1959) *The Presentation of Self in Everyday Life*, Doubleday, New York.

Goffman, E. (1961) *Asylums*, Anchor Books, New York.

Goffman, E. (1963) Stigma: Notes on the Management of Spoiled Identity, Anchor Books, New York.

Goffman, E. (1967) *Interactional Ritual*, Anchor Books, New York.

Hann, I-H., K-L. Hui, T.S. Lee, and I.P.L. Png (2002) "Online Information Privacy: Measuring the Cost-Benefit Tradeoff", *Proceedings of the Twenty-Third International Conference on Information Systems*, Barcelona, Spain, December 15-18.

ICCPR (1996) "The International Covenant on Civil and Political Rights", http://www.unhchr.ch/html/menu3/b/a_ccpr.htm

Johnson, Allan (1997) The Forest and the Trees: Sociology as Life, Practice, and Promise, Temple University Press: Philadelphia, Pennsylvania.

Kuhn, T.S. (1970) *The Structure of Scientific Revolution*, 2nd Edition, University of Chicago Press: Chicago.

Kuo, F.Y. and M.H. Hsu (2001) "An Investigation of Volitional Control in Information Ethics", *Proceedings of the 22nd International Conference on Information Systems*, New Orleans, USA, pp. 261-270.

Langford, D. (2000) (ed) *Internet Ethics*, MacMillan Press: London/New York.

Lee, A. S. (1991) "Integrating Positivist and Interpretive Approaches to Organizational Research", *Organization Science*, (2)4, pp. 342-365.

Lessig, L. (1999) *Code and Other Laws of Cyberspace*, Basic Books: New York.

Lin, C. (2003) "Self-Regulation Mechanisms in the Practice of Information Privacy", PhD Thesis, National Sun Yat Sen University, Taiwan.

Liu, C. and K.P. Arnett (2002) "Raising a Red Flag on Global WWW Privacy Policies", *Journal of Computer Information Systems*, (43)1, pp. 117-127.

McFarlan, F.W. (1984) "Information Technology Changes the Way You Compete", *Harvard Business Review*, (62)3, pp. 98-103.

Malone T.W., J. Yates and R.I. Benjamin (1987) "Electronic Markets and Electronic Hierarchies", *Communications of the ACM*, (30)6, pp. 484-497.

Meller, P. (2003) "Microsoft to Alter Online System to Satisfy Europe", *The New York Times*, January 31st.

Milberg, S.J., H.J. Smith, and S.J. Burke (2000) "Information Privacy: Corporate Management and National Regulation", *Organization Science*, (11)1, pp. 35-57.

OFPC (2001) “Privacy and the Community' Office of the Federal Privacy Commissioner”, Sydney, http://privacy.gov.au/publications/rcommunity.html#3.5

Parent, W.A. (1983) “Privacy, Morality, and the Law”, *Philosophy and Public Affairs*, (12)4, pp. 269-288.

Peng, M.W., Y. Lu, O. Shenkar and D.Y.L. Wang (2001) “Treasures in the China House: A Review of Management and Organizational Resarch on Greater China”, *Journal of Business Research*, (52)2, pp. 95-110.

Porter, M.E. (1985) “How Information Gives You Competitive Advantage”, *Harvard Business Review*, (63)14, pp. 149-160.

Scheibal, W.J. and J.A. Gladstone (2000) “Privacy on the Net: Europe Changes the Rules”, *Business Horizons*, (43)3, pp. 13-18.

Schneider, S.C. and J.-L. Barsoux (1997) *Managing Across Cultures*. London: Prentice Hall.

Schoeman, F.D. (1984) *Philosophical Dimensions of Privacy*. Cambridge: Cambridge University Press.

Smith, H.J. (2001) “Information Privacy and Marketing: What the U.S. Should (and Shouldn’t) Learn From Europe”, *California Management Review*, (43)2, pp. 8-33.

Smith, H.J. (1993) “Privacy Policies and Practices: Inside the Organizational Maze”, *Communications of the ACM*, (36)12, pp. 105-132.

Smith R.E. (2002) “Compilation of State and Federal Privacy Laws”, Privacy Journal, http://www.privacyjournal.net/work1.htm.

Tam, E.C., K.L. Hui and B.C.Y. Tan (2002) “What Do They Want? Motivating Consumers to Disclose Personal Information to Internet Businesses”, *Proceedings of the 22nd International Conference on Information Systems*, Barcelona, Spain, December 15-18.

UDHR (1948) Universal Declaration of Human Rights, http://www3.itu.int/udhr/

ABOUT THE AUTHORS

Robert Davison is Associate Professor in the Dept. of Information Systems at the City University of Hong Kong. He is editor-in-chief of the *Electronic Journal of Information Systems in Developing Countries* and an associate editor of the *Information Systems Journal*. He edits several Web pages for ISWORLD, including: Virtual Teams, Professional Ethics, Global IT Management and IT in Developing Countries. His recent work is published in *Communications of the ACM*, the *Information Systems Journal*, *IEEE Transactions on Engineering Management* and *Information Technology & People*. He recently completed editing a special section of the *Communications of the ACM* on Global Applications of Collaborative Technology, and a special issue of the *IEEE Transactions on Engineering Management* on Cultural Issues and IT Management. His current work involves an exploration of virtual teams in educational contexts, and an ongoing interest in applying Action Research in organizational problem solving.

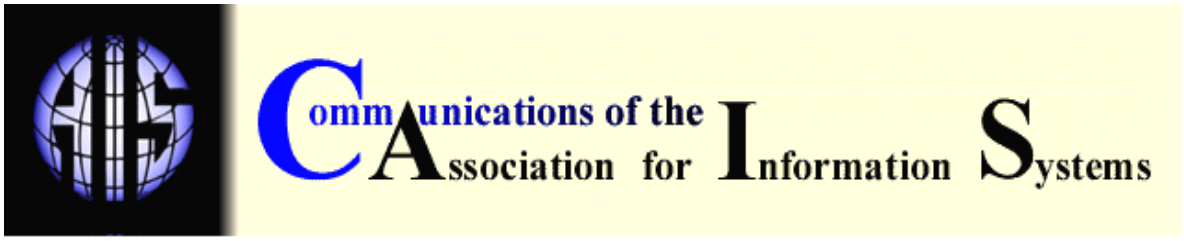
H. Jeff Smith is Professor at the Babcock Graduate School of Management, Wake Forest University. He is a D.B.A. from Harvard University. He worked for the International Business Machines Corporation for several years in software development. His research focuses on the societal reactions to strategic uses of information technology. His research appears in *California Management Review, Communications of the ACM, Harvard Business Review, MIS Quarterly, Organization Science, Sloan Management Review,* and in other journals. His book, *Managing Privacy: Information Technology and Corporate America*, published by the University of North Carolina Press, received the 1994 Donald

McGannon Book Award for Social and Ethical Relevance in Communication Policy Research.

Roger Clarke is a consultant in e-business, information infrastructure, and dataveillance and privacy. During his 30 years in the IS profession and discipline, he migrated from technical matters and the management of commercial software development, to an emphasis on strategic and policy aspects of information and information technology. He regrets that the discipline is still resisting the policy perspective. He holds a doctorate from the Australian National University. Following 5 years in Europe, he spent 1984-95 as a senior academic. He continues to publish in refereed outlets and to supervise postgraduate candidates, and sustains his academic associations through several visiting positions.

Duncan Langford lectures in Computing at the University of Kent at Canterbury, UK. Dr. Langford specialises in the relationship between computing and professional issues, and is regarded as an international expert in the field. Apart from many academic papers, his publications include *Practical Computer Ethics* [McGraw Hill, 1995] and *Business Computer Ethics* [Addison Wesley, 1999]. *Internet Ethics*, [2000], was published in the USA by St Martin's Press, and elsewhere by Pearsons (MacMillan).

Bob Kuo received his Ph.D. in information systems from the University of Arizona. He was a faculty member in information systems at the University of Colorado at Denver from 1985 to 1997 and is currently a professor of information management in the National Sun Yat Sen University, Taiwan. Bob's research interests include information ethics, cognition and learning in organizations, and human-computer interactions. His articles are published in *Communications of the ACM, MIS Quarterly, the Journal of Business Ethics, Information & Management, The Journal of Systems and Software, and Decision Support Systems.*



ISSN: 1529-3181