Background Paper for the Globalization of Personal Data Project International Survey on Privacy and Surveillance

Elia Zureik, Lynda Harling Stalker and Emily Smith

> Guarantees of privacy, that is, rules as to who may and who may not observe or reveal information about whom, must be established in any stable social system. If these assurances do not prevail – if there is normlessness with respect to privacy – every withdrawal from visibility may be accompanied by a measure of espionage, for without rules to the contrary persons are naturally given to intrude upon invisibility (Barry Schwartz, "The Sociology of Privacy," *American Journal of Sociology*, Vol. 73, 1968).

Introduction

In line with our plan to hold a workshop in November, 2006 to discuss the findings of the Globalization of Personal Data (GPD) project's international survey on privacy and surveillance, we have prepared this background paper and appended to it the survey questionnaire. There three main components to this background paper: first, to outline the various dimensions of privacy and the rationale for its empirical treatment as a key component of the GPD project that is being carried out at Queen's University; second, to provide an overview of ways to study privacy by means of public opinion research; third, to discuss the problems associated with the cross-national study of privacy, and ways to deal with them.

Dimensions of Privacy

What is Privacy?

There is no consensus on the precise definition of privacy; as analyzed by Daniel Solove (in Taipale 2003), the literature on privacy seems to cluster around the following six dimensions: (a) the right to be let alone; (b) limited access to the self; (c) secrecy; (d) control of personal information; (e) personhood; and (f) intimacy. This definition extends the original four-way definition (solitude, intimacy, anonymity and reserve) provided by Alan Westin who says,

> Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, whether in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve. The individual's desire for privacy is never absolute, since participation in society is an equally powerful desire. Thus each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to

> others, in light of the environmental conditions and societal norms set by the society in which he lives. The individual does so in the face of pressures from the curiosity of others and from the process of surveillance that every society sets in order to enhance its societal norms (1967: 7).

As remarked by Anthony Giddens, privacy has two aspects to it: "privacy as the 'other side' of the penetration of the state, and privacy as what may not be revealed" (1991: 153). Irving Goffman's exploration of privacy, it can be said, belongs to the second aspect of Giddens's definition. The first is connected with modernity and the rise of the nation-state and civil society. Although civil society provided protection against encroachment by the state on the private domain, the state and civil society continue to exist in a state of tension, particularly in times of national crises such as the events of 11 September, 2001. Here Westin (2003) and Giddens seem to be in agreement. For Westin, privacy ought to be considered at the political and the socio-cultural/organizational spheres.

Why Privacy?

As was made clear in the opening quotation from Schwartz's essay, privacy serves to stabilize the social system. But privacy serves personal ends as well. In seeking an answer to the question "why privacy?" Introna (1997) invokes ontological and existential arguments. Not only does privacy define the "context" in which people interact, it is also linked to intimacy by providing "moral capital" for sustaining human relationships. Borrowing from Goffman's *The Presentation of Self in Everyday Life* (1959), Introna locates the possibilities of enactment and management of social roles in "our ability to control who has access to us, and who knows what about us" (1997: 267). This is why many writers consider privacy as a requisite to autonomy for "without privacy there would be no self" (Introna, 1997: 269).

In a highly individualistic society such as ours, privacy is linked to individual rights, at times at the expense of collective and communitarian rights. As argued by Amitai Etzion (1999) and others (Bennett and Raab, 2006), the exercise of privacy has to be weighed against societal needs and the common good. This is why privacy can never be absolute.

Originally, the study of privacy was linked to urbanization and the emergence of mass society. With the flourishing of modernity the desire for privacy was pursued at the expense of participation in collective life. Richard Sennett (1998) and Christopher Lasch (1995) lamented the decline of public life and its transformation into a privatized form that reflected preoccupation with the self at the expense of involvement in public affairs. Here privacy is conceived in an individuated fashion, and is reflective of alienation and seclusion from public life. This latter theme appears in David Riesman's *The Lonely Crowd* (1950), Vance Packard's *A Nation of Strangers* (1972), and more recently in Robert Putnam's *Bowling Alone* (2000). It was the philosopher Hannah Arendt who, close to half-century ago, warned against "the cult of privacy [that] rests on an individualist conception of society" (1959: 70).

The task facing policy makers is how to balance individual needs for privacy against society's requirements, bearing in mind, as Charles Raab (1999) points out, that

the "balancing process" is fraught with problems. It is difficult to establish a "level playing field" in which privacy values are able to counter legislative and bureaucratic attempts at limiting the introduction of privacy protection measures. What is needed, he argues, is a multifaceted approach to privacy protection that relies on "regulation and self-regulations," and aims at educating the public, and making use of privacy enhancing technologies (see also Bennett and Raab, 2003). Priscilla Regan (2003) argues forcefully that privacy is not only an individual attribute, but also a common good on three counts: privacy is a "common value" to which each of us subscribes in varying degrees; privacy is a "public value" since it is a requirement for democratic practices at the political system level; and privacy is increasingly acquiring a "collective value" due to the pervasive influence of technology on the community as a whole.

Thus privacy is a means to an end; at the socio-cultural and psychological level it is the means for self-realization and ontological autonomy. At the political level, privacy is promoted as an antidote to state interference. In referring Westin's work, Stephen Margulis (2003) cites four functions of personal privacy. It provides for:

(a) personal autonomy and the desire to avoid being manipulated;
(b) emotional release and management of psychological and physical stress;
(c) self-evaluation which refers to one's need to integrate experience meaningfully; and
(d) a certain amount of protection to communication, which in turn defines interpersonal boundaries and for sharing information with others whom we trust.

Privacy with Regard to What?

Privacy violation, Gary Marx (2001) argues, implies transgressing **four borders**: natural borders, social borders, spatial and/or temporal borders, and ephemeral or transitory borders. This is akin to the definition provided by Robert Smith, editor of the *Privacy Journal*, who sees privacy as "the desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves" (cited in Privacy and Human Rights 2003). These, in turn, are equivalent to the four dimensions of privacy that are listed in the annual report *Privacy and Human Rights 2003: An International Survey of Privacy Laws and Developments* (Privacy International and Electronic Privacy Information Center, 2003). According to the report, the study of privacy encompasses **information privacy**, **bodily privacy**, **privacy of communication**, and **territorial privacy**. Although these are different facets of privacy and involve separate methods of data collection, they all can be cross-referenced through the convergence of information and communication technologies to construct profiles of people. Thus through data mining technique, bodily, territorial, informational and communicational data can be converted and merged to construct a digitized individual profile (See also Caryn Mladen2003). Whether practiced by the private or public sector, this merging of data is the basis for social profiling which is considered by David Lyon (2003) and others to constitute privacy violation on two counts. First, personal

information that was collected for one purpose is being used for another; second, data are merged from various sources to construct or infer behavioral patterns of subjects.

Ways of Studying Privacy

What to Look for in the Study of Privacy?

Margulis makes the point that although secrecy and privacy differ in certain respects, both revolve around controlling access and processes (of how information, possessions and space are managed), and as types (of privacy), and as functions (of privacy). The main difference between secrecy and privacy is that the management of the former is invested with greater emotional and cognitive efforts than privacy is. Secrecy is propelled by intentions to keep certain individuals, groups and organizations from penetrating the boundaries of the self. Our interest is mainly in the study of privacy.

Current, empirical and legal study of privacy has expanded significantly to include knowledge about (a) **awareness** of existing technological, legislative, and organizational means in the private and public sectors to protect/enhance privacy, as well as to include/exclude individuals; (b) **reaction** to and **experience** with specific privacy protection measures; (c) impact of so-called **big events** on privacy issues, such as the events of 9/11; (d) increasing articulation of privacy and **national security,** at times at the expense of privacy; (e) attempts at **harmonization** of national, regional, and international standards of privacy; and (f) the **importance** of privacy for commerce and individual users of electronic communication and transactions.

The globalization of commerce, travel and communication has also meant the globalization of privacy. Beyond comparative analysis of privacy legislations in various countries, which is not our concern in this portion of the project (see Bennett and Raab, 2003), there is a dearth of systematic information that deals with cross-national attitudes to privacy. Not only that such a comparative approach is costly, but that the methodological and conceptual issues involved in researching cross-national attitudes to privacy are substantial. It is hoped that this project will throw some light on this matter.

Operationalization of Privacy

The systematic study of privacy spans at least four decades of empirical research. In the process of carrying out such research, various attempts were made to develop operational concepts of privacy. It may be argued that the pioneering work of Westin, in association with several public opinion firms in the United States, has furthered the study of privacy more than research conducted by anyone else. Oscar Gandy's (2003; 2006) comment (aimed in part at Westin's work) concerning the danger that these surveys will be used to confer legitimacy on political and corporate agendas in the pursuit of influencing the on-going privacy debate makes it all the more important to pay close attention to the types of questions used by pollsters when assessing public reaction to privacy issues, and the context in which these questions are asked. A main theme that runs through public opinion data operationalizes the concept of privacy along the following lines:

(A) Westin's dimensions of privacy regarding personal lives:

(a) Privacy as **Solitude:** to be "free from observation by others";
(b) Privacy **as Intimacy:** "small group seclusion for members to achieve a close, relaxed and frank relationship;
(c) Privacy as **Anonymity:** to enjoy "freedom from identification and from surveillance in public places and public acts";
(d) Privacy as **Reserve:** the "desire to limit disclosure to others; it requires others to recognize and respect that desire." (Margulis, 2003: 412).

As demonstrated elsewhere, public opinion surveys have operationalized these and other privacy components so as to give us a longitudinal view of attitudes to privacy, albeit in western countries.

(B) Assessment of threat to privacy comes from various sources:
(a) Law enforcement agencies;
(b) Other government agencies (use of ID cards; CCTV, biometrics)
(c) On-line business transactions;
(d) Off-line business transactions;
(e) Health care system;
(f) Educational institutions;
(g) Employers;
(h) Marketers.

(C) Gary Marx's (2006) ranking of personal data (financial, health, etc.) in terms of sensitivity.

(D) Westin's classification of "ideological positions" of consumers regarding informational privacy has resulted in a three-way typology:

(a) Fundamentalists;
(b) Pragmatists;
(c) Unconcerned.

(E) Citizen awareness regarding data protection measures;

(F) Experience with attempts to secure information about one's self.

Why Study Public Opinion?

It is customary to think of public opinion as indispensable to the legislative process in a democracy. While not denying the importance of public opinion for governance, it is equally important to be cognizant of the processes that shape and mold public opinion, and the extent to which public opinion truly reflects informed choice. In a recent article, Gandy (2003) makes the point that at times public opinion surveys about privacy have been driven by corporate and special interests, whose framing of the questions (with the aid of academics and privacy experts) have depicted a concerned but fragmented public that is willing to trade privacy for utilitarian benefits. From a policy angle, he argues, public opinion surveys about privacy have played an important role in

framing the debate among policy makers. As I will show below, Roger Clark (in Davison et al., 2003), another key researcher on privacy, concurs with this assessment.

Although this observation has been made with regard to public opinion research in general (Osborne and Rose 1999), it has special significance at times of national debates, such as those accompanying the widespread use of surveillance technology following the terrorist attacks on the United States on 11 September, 2001.

It suffices at this point to underscore the need to pay attention to context and design of the questionnaires, especially concerning individually and politically sensitive topics, by offering two examples from Canada.

First, consider a Canadian poll that was carried out by COMPAS in behalf of the National Post in 2003, and found its way to the deliberations of the Standing Committee on Citizenship and Immigration in Parliament that was in the process of assessing the adoption of national ID card. The survey asked, “Do you see the terrorist threat from Islamic extremists as more serious than most threats,” and “Should people in Canada who are accused of being terrorists have the same rights as accused criminals?” The Parliamentary Committee saw the contaminating effect of these loaded questions on subsequent answers and dismissed the survey because it “raised doubt about the usefulness of the response” (Canada 2003).

Consider another survey, this time carried out by EKOS in behalf of Citizenship and Immigration Canada (CIC). EKOS is an experienced polling organization that has pioneered the study of privacy issues in Canada. Its survey *Privacy Revealed* (1993) was one of the early, detailed explorations of public attitudes to privacy in Canada. On the eve of the Ottawa conference, it was commissioned by CIC to carry out a national survey that dealt with biometrics and the receptivity of Canadians to adopting ID cards in light of privacy concerns. The findings were presented at a high profile conference on biometrics and national ID cards that was held in Ottawa in October of 2003 under the sponsorship of CIC.

In examining the order of questions, the EKOS survey unwittingly tapped into the mind of the public an implicit association between immigrants and terrorism, even though national data in Canada show that immigrants have substantially lower crime rates than native-born Canadians. For example, the lead question in the survey asked if respondents thought there were “too many immigrants” in Canada, to which one-third answered in the affirmative. From there the survey proceeded to ask a battery of questions on terrorism, biometrics and national ID card. Although a minority of Canadians (around 12%) thought that Canada would be exposed to a terrorist attack, and fewer (2.5%) thought that they personally would be affected, around 45 per cent agreed with the statement that "there is a serious problem with groups supporting terrorist activity in Canada," and 61 per cent agreed to the statement that "given the potential of terrorism, the Government of Canada should be given special (extraordinary – parentheses in original) powers to deal with possible terrorism-related offences."

The upshot of this is that most Canadians are willing to sacrifice privacy through the use of biometrics for the sake of security, even though as the survey discovered only a minority (15%) of respondents knew what biometrics meant. The finding regarding the relationship between privacy, security and terrorism is not unique to Canada, but is found in other surveys in the United States, Britain, and several European countries.

The above examples revealed both the strength and weakness of public opinion research on privacy. The strength lies in the quick response with which commercial organizations respond to gauging public opinion reaction to external stimuli. In our case, interest in privacy is heightened as a result of two factors: the ubiquitous presence of information and communication technology in society, and the crisis following the terrorist attack of 11 September, 2001. But it is precisely this quick reaction to events which yields instantaneous attitudinal data that may not be stable over time. Unless one is able to examine public opinion data longitudinally, it is difficult to conclude with certainty about the stability of such attitudes. From the data examined in this paper, it is clear that the initial willingness of the public to compromise privacy rights for the sake of greater security has now diminished and been tempered with considerations weighing the tradeoff between privacy rights and perceptions of security.

Complex phenomena, and privacy is such a phenomena, are difficult to capture in their various nuances by means of single, close-ended questions. Cross-national data revealed that the public knows very little about the nature of the monitoring technology, and is equally uninformed about privacy legislations and their rights under such legislations. For this reason, it is crucial to pay attention at the outset to the research design and the interview instrument, so as not to collect data that is already known before hand and/or tap so-called "surface" opinions only. This is why qualitative research and the use of focus groups become important in contextualizing the research process.

Most of the research reviewed here has a "market" focus, since it is driven by corporate interests seeking to unravel consumer attitudes to privacy. This is particularly true in North America, although the globalization of business is extending interest in online privacy and its associated concerns governing financial transactions. As such there is little interest by polling organizations in fielding questions of theoretical value. For example, with regard to cross-national surveys it is important to relate the survey findings to the specific historical and cultural experience of the society in question. At a more general level, it is appropriate to enquire into the relationship between attitudes to privacy and political culture characteristics.

Finally, most of the research covered here lacks what I call an "empowerment" dimension, i.e., the differential effects of surveillance felt by different groups in society. In particular, how is privacy viewed with regard to vulnerable groups in society – the elderly, poor people, visible minorities, etc? As well, it is appropriate to assess the extent to which the public is willing to adopt anti-surveillance strategies in its encounter with governmental and corporate attempts at privacy invasion. These may not be easy topics to handle in an opinion survey, but it is worthwhile raising the issues and hopefully addressing them at the workshop.

Cross-National Study of Privacy

Why Conduct Cross-National Studies?

A few years ago, Colin Bennett remarked that "the lack of reliable cross-national data on citizen attitudes toward privacy would suggest a pressing need to commission surveys that allow more comprehensive and reliable inferences to be drawn. There is surely an unjustifiable imbalance in the survey data currently available" (1996:17; see also Bennett and Raab, 2006:). It is still the case that survey research on privacy is most

developed in North America - the United States in particular. However, we have seen constant expansion of privacy studies covering various facets and countries (which are mostly western). In large measure this increase has been due to the promotion of human rights, good governance and the establishment of privacy ombudsman offices in several countries. More significantly though, it is the spread of globalization that has spurred cross-national interest in privacy. First, state reactions to terrorism have been accompanied with national legislations to track down terrorist activities. These political initiatives triggered reactions from the public and privacy advocacy groups who saw in excessive government intrusion ominous threat to privacy protection. It is thus not surprising that recent public opinion surveys examining citizen attitudes to anti-terrorism legislation focused on privacy in the context of national security. Second, globalization is largely facilitated by the electronic flow of information across international borders. The sheer magnitude of transmission of financial and personal data has led to calls for developing proper means to safeguard informational privacy. Third, several public opinion surveys that dealt with the spread of electronic commerce have concluded that adequate privacy protection of personal data is a basic requirement mentioned by consumers for successful e-commerce, although Europeans more than Americans tend to leave it to government rather than business to regulate citizen privacy. In a world that is becoming increasingly connected, privacy ceases to be the exclusive concern of individuals and indeed single governments, and becomes also the global concern of regional and international organizations (the European Union and OECD, for example).

What Problems to Expect when Carrying out Cross-National Privacy Surveys?

The pitfalls in carrying out global research on privacy were highlighted by an international panel on *Information Privacy in a Globally Networked Society: Implications for Information Systems Research* (Davison et al. 2003). The problems spanned the following areas:

> "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"

Challenges of a general nature should be familiar to students of survey research. Issues of reliability and validity of the items in a cross-national research are important in controlling for measurement bias. Sensitivity of the topic and phrasing of questions are crucial here. How does one get honest responses from participants in a survey, if they themselves feel their answers might compromise them? This is crucial in societies where

the respondents are not accustomed to revealing intimate data about themselves, such as East European and some Latin American countries. Non-response bias due to non-randomness of those who do not respond may lead to biased samples that are different from the population composition originally envisaged in the sample design. Also, bias can be generated with non-response to certain questions in the survey.

For the sake of convenience and/or cost, researchers sometimes choose proxy samples to carry out their research, assuming that they are representative of the population. The Likert scale problematic is a familiar one. How does one insure that the ordinal scales used in questionnaire items are actually ranked meaningfully in an equidistant fashion cross-culturally? One should also keep in mind that Likert scales are not generally used in qualitative data, such as our focus group interviews.

Quality challenges that are specific to privacy-related surveys must consider privacy as an intervening or confounding variable. A low response rate can in itself be an indicator of people's privacy concerns. Can one assume that attitudes to privacy among those who answer the questionnaire are similar to those who did not respond, even if it is the case that the latter's refusal is due in part at least to placing high value on privacy? Because privacy means different things to different people and spans several domains, it is important that respondents be told by the interviewer the context of their attitudes to privacy that are being sought after. For example, Roger Clark suggests that researchers should distinguish between behavioural privacy, privacy of the person, communicational privacy, and privacy of personal data. In addition to cultural relativism which weighs heavily in cross-national investigations of privacy, Clark makes a connection between the media and its influence on public attitudes towards privacy, a point that was raised above by Gandy. According to Clark,

> Media reports (which for the most part reflect propaganda, public relations campaigns and controlled information flows from governments, government agencies, and corporations – parentheses in original) 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 politicization 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 D.C. the previous day (in Davison et. al, 2003: 345).

Another, equally useful study of cross-national research is written by the president of MORI, Robert Worcester, in collaboration with Marta Lagos and Miguel Basanez (2000). The paper is very useful because it is written by individuals who have substantial experience in carrying out international surveys. The paper talks to nitty-gritty problems faced in cross-cultural research of public opinion. The authors highlight the problems encountered in drawing up representative samples in regions where reliable frames for population count (such as census) are not available, where within country population heterogeneity (such as in Brazil) poses sampling problems, and where the problems of language and questionnaire translations across cultures are serious problems. Here the problem of meaning and lack of language equivalence across cultures becomes

challenging. In our case, for example, to what extent is the word privacy salient in East European countries, China and Mexico, compared to Canada and United states? Does privacy mean the same thing to people from different cultures? The authors suggest using reverse translation, i.e., telling what the word privacy means in so many words so as to make sure that the researcher is tapping equivalent meaning, even though the word as such is not part of the vocabulary of the country. Here is how the authors put it:

> In those cases [cross-cultural contexts] the word is translated into a phrase, and has to be analyzed as such. Back translations of questionnaires is a fundamental part of multinational, multilingual studies; many mistakes are made when this is not done, even when working in the same language…(p. 8)

Two additional problems are raised by the authors, and it is useful to mention them: one, concerns the use of semantic differential scales, and the other refers to the assumptions of cross-cultural comparability of socio-demographic indicators. We have alluded to the first problem earlier, but the authors add an interesting dimension to the relationship between culture and placement on a Likert-type scale. They note that in Latin America, it is culturally more comfortable for people to take a middle position so that they do not appear to be partisan. Thus a four-point scale produces higher non-response rates than a scale with uneven choices. It is also the case, however, that some would prefer a mid-point on the scale so as to "hide" one's true location. With regard to socio-demographic indicators, the problem raised by cross-cultural research is best illustrated when comparing cross-nationally income, education and occupational data. In many societies ranking data on income is problematic. Is a middle-income position in one country equivalent to a similar position in another country? What about those countries with thriving informal economies? How does one account for income distribution? Similarly, when ranking people by educational level, can one assume that the quality of education is comparable cross-nationally? In societies undergoing extensive political and economic transitions, such as East European and certain developing countries, the meaning of socio-demographic differentiation and ranking changes quickly across time. This change is also evident in regions within one country.

Anchoring Vignettes

Gary King *et al.* (2004) identified the need to ameliorate differences in cultural understandings while doing cross-cultural research. What these authors argue is the need to have a standard measure, or anchor, within a survey by which researchers can accommodate cultural differences. This is a two-prong form of survey research that provides a self-assessment question and then a question on the assessment of hypothetical others in situations along the same scale as the self-assessment. Scale anchors therefore allow for the interpersonal comparison to occur. The anchoring vignettes are useful for measuring abstract concepts like privacy. Through the use of third-person scenarios, we are able to discern cultural thresholds on a standard scale. King's idea underlying anchoring vignettes is to measure directly, and then subtract off, the incomparable portion. "Since the actual (but not necessarily reported) levels for the people in the vignettes are, by the design of the survey, invariant over respondents, the only reason

answers to the vignettes will differ over respondents is interpersonal incomparability" (King 2003). We can then take these thresholds and adjust self-assessments accordingly.

There are two key requirements for using anchoring vignettes. The first is that there must be response consistency. The self-assessment questions and vignette scenarios must be used in the same manner, with the same scale. The respondent must therefore use the self-assessment and vignettes in the same way. The second requirement is that there is vignette equivalence. There needs to be one vignette for every level within the scale. For our GPD survey, we have a self-assessment question with a four-point response scale and four vignettes that we believe correspond to each domain level.

Our anchoring vignettes focus on two key aspects of privacy: control over personal information, and respect of personal privacy by airport officials. These questions allow us to interrogate privacy as it relates to the actors central to this project – citizens, consumers, workers and travellers.

As one might expect, using anchoring vignettes can be a costly venture. This method adds to the translation cost, programming of the computer-assisted telephone interviews, and to the survey administration time. For this reason, we have heeded King *et al.*'s advice and did the anchoring vignettes using a sub-sample of fifty per cent for each set of vignettes. The self-assessment questions will however be asked of all participants. It is felt that this sub-sample will be sufficient to provide statistically significant data to develop the necessary thresholds for cross-cultural comparisons.

By using anchoring vignettes not only does this survey contribute to Surveillance Studies, but also to the literature on cross-cultural survey research and studies on public opinion polls.

Selection of countries

For this project, we made sure that the countries under investigation are politically and culturally diverse, while at the same time had significant ICT penetration to be able to speak to our concerns. The decision was made to look at Canada (English and French), United States, Mexico, Brazil, France, Spain, Hungary, China and Japan. These countries represent the spectrum of political models (communism, post-communism, socialism, democracy), economic status (developed, developing, and underdeveloped), and different regulatory policies governing internet use.

Cultural values and Triangulation

Cultural values are central to understanding how privacy and surveillance issues play out in our survey. It would be naïve to do cross-cultural / cross-national research without some understanding of how values shape people's perception and opinion on the subject. We have found that within sociology there is paucity of cross-cultural research on privacy. As such we have turned to the business literature on privacy and e-commerce to interrogate how cultural values play out in cross-cultural research.

The primary researcher in this area over the last number of years is Geert Hofstede (1980). He analyzed data gathered from IBM employees in 70 countries between 1967 and 1973 to interrogate values related to the workplace. Through his research, Hofstede developed four indices that are pertinent to our discussion of privacy:

1. Power Distance Index (PDI): Cultures that measure high on the PDI are more likely to tolerate greater power inequality between groups and are more comfortable with centralized power.
2. Individualism Index (IDV): This looks at the distinction between collectivist and individualist cultures.
3. Masculinity Index (MAS): High scores here indicate the culture is more tolerant of gender inequality, and places a greater emphasis on material success.
4. Uncertainty Avoidance Index (UAI): UAI measures the resistance to change within a culture. The higher the UAI score, the higher the resistance to change.

Other researchers have taken Hofstede's indices to examine questions that revolve around privacy and business interests. Milberg *et al.* (2000) found positive associations for PDI, INV, and MAS with the overall effect of cultural values on information privacy across cultures. The higher the score on these indices, the higher the concern for information privacy. There was a negative association for UAI with the overall effect of cultural values; therefore the more resistant to change a culture is the less likely there are concerns for information privacy. This is perhaps due to the fact that cultures with high UAI want more government regulation to mitigate the likelihood of risk and change. More regulation might mean that the perception of information privacy is being taken care of by the government. Bellman *et al.* (2003) also took Hofstede's indices to explore information privacy and the concern of unauthorized access. He found that while cultural values are influential, their effect was the opposite of what Milberg *et al.* concluded. Bellman and his collaborators found that higher scores in PDI, IDV, and MAS and lower scores in UAI indicated lower overall concern about information privacy and unauthorized access. With such contradictory results, one wonders whether Hofstede's cultural values are relevant to discussions on privacy. We would argue that they at least provide a means to conceptually talk about cultural values, and our survey will be able to add to the debate about how cultural values shape opinions on privacy.

To further augment our understanding of cultural values we turn to the World Values Survey (WVS). The WVS is a survey that has been conducted since 1981 in four waves throughout approximately 80 nations. While surprisingly excluding questions that deal with privacy and surveillance, we are able to take questions about trust, governance, authority, relationships and gender from the WVS. This allows us to see how countries' scores on these values relate to their attitudes toward privacy and surveillance. We will be able to hypothesize whether or not different cultural values elicit different attitudes toward privacy.

Focus groups

In 2004, the GPD project conducted focus groups in the nine countries of interest. The choice of participants in the groups were based along the lines of the four actor categories – workers, consumers, citizens, and travellers – to participate in a guided discussion on privacy. Questions were asked that dealt with privacy issues in general, and then those that were specific to the actors present.

The focus groups, within which there were approximately 15 participants in each, were recruited and administered by Ekos Research Associates in North America and Ipsos in the remaining countries. These firms have experience not only in focus group

research, but are well known for the public opinion polling they do on privacy related issues. The participants were selected in order to maintain a broad demographic range, and to meet requirements for representation from each of the actor groups. Each focus group was video taped, transcribed into English, and summaries were prepared on the findings. These summaries are available upon request.

Focus groups were conducted for a couple of reasons. First, the focus groups help to identify key concerns about privacy present in the various countries. It is apparent that different types of privacy are important in various degrees in the countries. For example, at the end of each focus group, the participants were asked to fill out a ranking form to indicate their perception of the importance and threat for each type of privacy. The following two tables summarize the results.

Table 1: Degree of importance for each type of privacy by country

Type	Canada	U.S.A.	Mexico	Brazil	France	Spain	Hungary	China	Japan
Bodily	2.53	**2.30**	**2.06**	2.21	3.41	2.05	2.95	**1.92**	2.65
Comm.	**2.08**	**2.30**	2.78	**1.74**	2.53	**1.95**	**1.95**	2.38	2.65
Info.	2.27	2.35	2.50	1.84	2.24	3.05	2.75	2.96	2.95
Territorial	2.75	3.05	2.67	2.11	**1.82**	2.95	2.35	2.73	**1.75**

1 = most important 4 = least important

Bold indicates most important within the country

Table 2: Degree of threat for each type of privacy by country

Type	Canada	U.S.A.	Mexico	Brazil	France	Spain	Hungary	China	Japan
Bodily	2.80	3.35	2.83	**1.63**	2.71	2.25	2.75	2.42	2.90
Comm.	2.20	2.10	2.22	1.89	2.35	**2.05**	**1.80**	**2.38**	2.00
Info.	**1.53**	**1.35**	**1.89**	1.89	**1.88**	2.20	2.30	2.54	**1.50**
Territorial	2.88	3.10	3.06	2.58	3.06	3.50	2.15	2.69	3.60

1 = most important 4 = least important

Bold indicates most important within the country

Knowing this assisted in focusing the questions in the international survey in the right areas. Our questions are geared more toward concerns about information privacy, as this was perceived to be the most under threat despite having a lower degree of importance.

The analysis of the focus groups also allows us to hypothesize what will come out of the survey. The information gathered in this setting gives us, if not a firm idea of what to expect, at least a general notion as to how each country will respond to questions about privacy.

We can then use this information to triangulate the results. With Hofstede's cultural values, the World Values Survey, and the international survey we are able to present a well-informed cross-cultural picture of privacy and related concerns. With the qualitative data the focus groups provide, we can better understand and explain the results we get from the quantitative international survey. The anecdotal discussions in the focus groups help to provide the cultural and social milieux, as well as current debates happening in the country, to know how the survey results pertain to the countries.

Technology awareness and familiarity

As our survey asks questions that require a level of understanding about technological uses, we have looked to see to what degree basic ICT technology diffused in each country. The following table presents penetration rates for personal computers, land lines and cell phones.

Table 3: Information and communication technology penetration by country

	Personal computers / 100 inhabitants (2002-2003)	**Main telephone lines / 100 inhabitants (2003)**	**Cell phone subscribers / 100 inhabitants (2003)**
Brazil	7.5	22.3	26.4
Canada	48.7	65.1	41.9
China	2.8	20.9	21.5
France	41.7	56.4	69.6
Hungary	10.8	34.9	76.9
Japan	38.2	47.2	67.9
Mexico	9.8	16.0	29.5
Spain	19.6	43.4	90.9
U.S.A.	68.7	62.4	54.6

Source: *The global competitiveness report, 2005-2006*. World Economic Forum

In this table we see three groupings. The first are the developed countries of Canada, France, Japan and U.S.A. These countries all have high penetration of basic ICT. This bodes well for the survey, in that there is an inferred level of awareness and familiarity from such high levels. The next grouping would be Hungary and Spain. These countries' levels of penetration increase as we move across the chart, with these countries having the greatest rate of cell phone subscription. Again, this speaks to an expected awareness of and familiarity with many different technologies. Particularly as cell phones are becoming increasingly sophisticated the respondents to our survey in Spain and Hungary will more than likely demonstrate an awareness to the technological issues we are addressing. The final group is Brazil, China, and Mexico. Across the board, we see these developing countries as having low levels of technology penetration. It becomes more of an issue in these countries with regards to our survey. Part of the way we will overcome this is by using urban samples. It is anticipated that in urban areas there is greater access to technology than in rural ones. We will see if this plays out in the survey results.

One of the critical technologies we are interested in is the Internet. Below is a table of Internet penetration and growth across the nine countries.

Table 4: Internet penetration and growth in usage

Country	% of population using the internet 2005 (internet penetration)	Percentage of growth of internet users (2000-2005)
Canada	67.9	72.4
USA	68.1	113.8
Mexico	16.2	526.6
Brazil	14.1	418.0
France	43.0	208.4
Spain	38.7	218.2
Hungary	30.3	326.6
China	8.5	393.3
Japan	67.2	83.3

Source: http://www.internetworldstats.com

Of our nine countries, eight are in the top twenty of internet users worldwide (Hungary is the only one not listed).

Table 5: Percentage of world internet users and ranking

Country	% of world net users (2005)	Ranking
USA	20.0	1
China	10.9	2
Japan	8.5	3
France	2.6	9
Brazil	2.5	10
Canada	2.2	12
Spain	1.7	14
Mexico	1.7	15

Source: http://www.internetworldstats.com

From these two tables we can hypothesize that there is a fair amount of familiarity, if not awareness, when it comes to the Internet. This familiarity is growing, particularly in Mexico, Brazil and China. While the penetration rate in these countries is substantially lower than others, the fact that there is a large population base to draw from means that the actual number of people using the Internet is higher than one might expect. We can see this in the countries' rankings on a worldwide level. This bodes well for people's ability to answer our questions regarding privacy and the internet.

As there is great familiarity and availability to internet among our countries, we need to heed the advice of DiMaggio *et al.* (200?) that instead of talking about the digital divide, a concept with historical roots in landline telephones, we need to talk about "digital inequality." These authors note that having access is not enough to ensure equality of access to information. DiMaggio and his colleagues highlight four dimensions of digital inequality:

1. Technology means: the capacity of the technology used and the means to access highspeed internet vs. dial-up internet
2. Autonomy: the freedom to use an internet to gather information can be mitigated by social economic status, demography, and situational factors
3. Skill: having the required skill-set to not only retrieve information but also to do so in a timely manner
4. Social support: a user not only needs to have professional technical support but there must be a network of family and friends to disseminate skills, technical knowledge, and provide emotional reinforcement.

When all taken together the hypothesis states that the greater your access is to these four components, the more likely the users' objectives will be met, both directly and indirectly, and human and social capital will be increased. As one's social capital increases their life chances increase as one is able to access necessary information with ease.

Questions Addressed by the Survey

In the conclusion to his stocktaking paper on public opinion and privacy research, Colin Bennett (1996) posed several questions which, if pursued in cross-national research, will enrich our knowledge of privacy, and at the same time highlight comparisons bearing on the issue of privacy regulation. As pointed out earlier, researchers in business schools have been pioneers in cross-national studies of privacy from consumer and corporate perspectives. For example, Steven Bellman and his associates hypothesized that "cross-cultural values will be associated with differences in concern about information privacy" (2003:7). Drawing upon Bennett's, the work of Bellman et al., among others, and our own research it is possible to make the following observations in the form of questions in search of answers. Our international privacy survey will shed light on these questions:

(a) How do demographic variables pan out in cross-national surveys of privacy? Do we expect to find that cross-national variations will remain when controlling for various demographic variables, such as education, gender, race, age, income, etc.? How will cross-national variations in attitudes to privacy compare to within-country variations?
(b) To what extent can one explain variations in responses to privacy items on the basis of political culture variables? In other words, is the attitude to privacy shaped by the unique historical experience of the country in question?
(c) Is it the case that countries which experienced authoritarian regimes orient themselves differently to privacy than those living in liberal-democratic states, and in what ways?
(d) Similarly, how will the cultural distinction between collectivist and individualist orientations at the societal level manifest itself in terms of attitudes to privacy?
(e) How do individuals in cross-national surveys rank-order privacy as a value relative to other values, including the value of human rights?

(f) Is the attitude to privacy contingent upon orientations to technology generally, i.e., the more individuals understand the technology the more likely that they will endow technology with elements of trust in terms of protecting their privacy?
(g) Do people know, and do they care to know, what happens to the information that is routinely collected about them? Or, is their concern directly correlated to the type of personal information discussed (health, financial, etc.)
(h) How familiar is privacy legislation to citizens, and the extent to which they are likely to make use of such legislation?
(i) Are internet users aware of privacy policies (so-called privacy seals) that are posted on the web sites of various public and private sector organizations? What do users think of these policies? Do they consider them adequate measures of privacy protection?
(j) What is the extent and nature of the relationship (correlation), if any, among the four components of privacy to which we referred above, e.g., informational, territorial, bodily and communicational privacy? Is the saliency of these privacy components the same cross-nationally?
(k) Since the media has great influence on public attitudes to key issues in the public domain, and privacy is one of them, should we not ask about respondents' perceptions of the role of the media and their sources of information about privacy issues?
(l) Since our concern in this project is with four different types of actors (as citizens, travelers, employees, and consumers), do people in different countries orient themselves differently to privacy, depending on the role(s) they occupy?
(m) Does the extent to which consumers are willing to trade information about themselves in return for personal benefits of material or non-material kind vary cross-nationally?
(n) What do consumers think of fair information practices as they relate to the three main justice perspectives discussed in the literature: distributive, procedural and interactional?
(o) What are workers' attitudes toward workplace surveillance? What forms of monitoring do workers perceive to be appropriate and what forms do they feel invade their privacy? Is there variation not only across cultures but also across occupations and income levels?
(p) Privacy has almost been twinned in policy and media discourse with security. Do people in various countries perceive it in this manner, or do they consider it to be a uniquely American concern that is less relevant to their situation?
(q) What do citizens think of the practice whereby governments provide the United States with advance information on travelers destined for the United States? To what extent could this be considered a sign of compromising individual privacy and national sovereignty?

Appendix I
Themes Covered in the Globalization of Personal Data Survey on Privacy and Surveillance

Below is a list of themes that are covered in the GPD survey, along with their corresponding question numbers in the questionnaire:

Knowledge of technology and laws

- Level of knowledge about technologies, including the internet, Global Positioning System (GPS), Radio-Frequency Identification (RFID) tags on consumer products, Closed Circuit Television (CCTV) in public spaces, biometrics or facial and other bodily recognition and data mining of personal information (1)
- Level of knowledge about laws that protect personal information in government departments and private companies (3)
- Ranking the effectiveness of laws at protecting personal information held by government departments and private companies (4)

Control over personal information

- Extent of say in what happens to personal information (2)
- This is the anchor for vignette questions (29, 30, 31, 32)

Trust: government and private companies

- Level of trust in government to balance between national security and individual rights, when it comes to the privacy of personal information (5)
- Level of trust in private companies to protect personal information (6)

Actions

- Steps individuals have taken to protect their personal information (7), including:
    - Refusing to give information to businesses or government agencies because they thought it was not needed
    - Asking a company to remove them from any marketing lists, not to sell their name and address to another company, or to see what personal information they have about them in their consumer records
    - Asking a business about their policies on the collection of consumer information
    - Purposefully giving incorrect information to a marketer or government agency
    - Reading on-line privacy policies at websites when making a purchase from a private company or at a government website when sending them information electronically

Experiences

- Experiences with surveillance measures (8), including:
    - Detention at border checkpoints resulting in being searched, not being able to board an airplane, or being denied entry into a country
    - Being the victim of identity theft or of credit card fraud
    - Personal information being monitored by a government agency, an employer or being sold by a commercial business

National ID cards

- Extent of agreement or disagreement that everyone should have a government-issued national ID card that must be carried at all times (9)
- Effectiveness of efforts to protect citizens' personal information from disclosure that would be held in a national database for ID cards (10)

Internet

- Worry about privacy implications when providing personal information on websites (11)
- Who should have the most say over how companies track personal information online: government, companies that run the websites or people who use the websites (12)

Media coverage

- The amount of media coverage respondents have heard or seen about the safety of personal information (13)
- Whether the media pays more attention to stories about terrorism or government violation of personal privacy (14)
- Whether the media pays more attention to stories about terrorism or private sector violation of personal privacy of consumers (15)
- Which groups receive the most and least amounts of media coverage about privacy of personal information (16)

Terrorism and security

- Whether laws protecting national security are intrusive on personal privacy (17)
- (Overlap with trust question) Trust in government to balance between national security and individual rights (5)

Information sharing

- Appropriateness of government agencies sharing citizen's personal information with third parties, such as other government agencies, foreign governments, and private sector (18)
- Appropriateness of private sector organizations sharing or selling customer personal information with third parties, such as the national government, foreign government, and other private sector organizations (19)

CCTV

- Effectiveness of CCTV in reducing crime, in the community and in stores (20)

Actors: Worker, Traveller, Consumer

- Worker:
  - To what extent employers should be allowed to electronically monitor their employees with surveillance cameras and to read the e-mails their employees send or receive on the employer's computers (21)
  - To what extent it is appropriate for an employer to share employee personal information with third parties, such as the government or the private sector (22)
- Traveller:
  - To what extent privacy is respected by airport and customs officials when travelling by airplane (23)- the is the anchor for vignette questions 33, 34, 25, 26
  - Whether the government has the right to collect personal information about travellers (24)
  - Whether the government should be able to share travellers' personal information with foreign governments (25)
  - Acceptability for airport security officials to give extra security checks to visible minorities (26)
- Consumer:
  - The number of rewards programs that respondents collect points or rewards from (27)
  - Acceptability of businesses to use information from customer profiles to inform respondents of products or serves that they think would interest them (28)

Vignettes

- Group A: question 29-32- vignette examples related to anchor question 2 on the extent of say in what happens to personal information, with question 30 being the most extreme example, 32 the second most extreme, 29 the second least extreme, and 31 the least extreme example
- These questions relate to the level of say over personal information use in various contexts, including question 29 about the amount of personal information required by a company in applying for a customer loyalty card to receive discounts, 30 involving a government database of detailed personal biometric information held on citizens used to search for terrorist activity, 31 about customers in a department store paying by cash and not exchanging any personal information in their transaction and 32 on the merging of various government databases of personal information held on citizens to search for terrorist activity
- Group B: question 33-36- vignette examples related to anchor question 23 on the extent that privacy is respected by airport and customs officials when travelling by plane, with question 35 being the most extreme response, 34 the

second most extreme, 33 the second least extreme and 36 the least extreme example

- These questions are about the extent to which privacy is respected in various scenarios by airport and customs officials to passengers that are travelling out of the country, 33 relates to a traveller having their baggage checked before boarding the plane, 34 involves an individual being singled out and having a metal detecting wand passed over them before boarding the plane, 35 is on racial profiling being used to ask very detailed questions about a traveller including physical searches before travel and 36 is about a traveller being permitted to board a plane by showing their passport

Demographic questions

- Number of times travelling by air in the past year, within and outside the country (37) (to determine travellers)
- Purchase of product over internet in past year (38) (to determine online consumers)
- Contact with local, state or national government in the past year by various means (39) (to determine citizen)
- Computer use in the past 6 months in various contexts: at home, at work, in a public place (39b)
- Internet use in the past 6 months in various contexts: at home, at work, in a public place (39c)
- Year born in (40) (age)
- Highest level of education completed (41)
- Current employment status (42)
- Current occupation of employed (43) (to determine workers)
- Annual household income (44)
- Language spoken at home (45)
- Ethnicity (46)
- Race (47)
- Language of interview (48)

References

Arendt, Hannah. 1959. *The Human Condition*. Chicago: University of Chicago Press.

Bellman, Steven, Eric J. Johnson, Stephen J. Kobrin and, and Gerald L. Lohse. 2003. *International Differences in Information Privacy Concern: Implications for the Globalization of Electronic Commerce*, May 7, 2003. Available at: www.cebiz.org/research/privacy_security/index.html

Bennett, Colin J. and Charles D. Raab. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective*. The MIT Press: Cambridge. [2nd and updated edition from 2003]

Bennett, Colin J. and Charles D. Raab. 2003. *The Governance of Privacy. Policy Instruments in Global Perspective,* Cornwall, Britain: Ashgate.

Bennett, Colin J. 1996. *Frequently Asked Questions about Privacy: A Comparative Analysis of Privacy Surveys,* University of British Columbia, unpublished manuscript.

Canada. 2003. *A National Identity Card in Canada?,* Report of the Standing Committee on Citizenship and Immigration, Joe Fontana, Chair, Available at: http://www.parl.gov.ca

Culnan, Mary and Robert J. Bies. 2003. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues*, Vol. 59, No. 2, pp. 323-342.

Davison, Robert M., Roger Clark, H. Jeff Smith, Duncan Langford, and Feng-Yang Kuo. 2003. "Information Privacy in a Globally Networked Society: Implications for Information Systems Research," *Communications of the Association for Information Systems*, Vo. 12, pp. 341-365.

DiMaggio, Paul, Eszter Hargittai, Coral Celeste, and Steven Shafer. n.d. *From Unequal Access to Differentiated Use: A Literature Review and Agenda for Research on Digital Inequality.* A Report prepared for the Russell Sage Foundation.

EKOS Research. 2003. *Canadian Attitudes Towards Biometrics and Document Integrity*, survey results presented at the Citizenship and Immigration Canada Forum, Ottawa, 7-8 October 2003.

EKOS Research. 1993. *Privacy Revealed: The Canadian Privacy Survey*, Ottawa: EKOS Research Associates.

Etzioni, A. 1999. *The Limits of Privacy*, New York: Basic Books.

Gandy, Oscar H. 2003. "Public Opinion Surveys and the Formation of Privacy Policy," *Journal of Social Issues*, Vol. 59, No. 2, pp. 293-299.

Gandy, Oscar Jr. 2006. "Data Mining, Surveillance and Discrimination in the Post-9/11 Environment", in Kevin D. Haggerty and Richard V. Ericson (Eds.) *The New Politics of Surveillance and Visibility.* Toronto: University of Toronto Press, pp. 363-384.

Giddens, Anthony. 1991. *Modernity and Self-Identity*, Cambridge: Polity Press.

Goffman, Erving. 1959. *The Presentation of Self in Everyday Life*, Garden City, New York: Doubleday.

Hofstede, Geert. 1980. Cultures Consequences: International Differences in Work-Related Values. Beverly Hills, Calif.: Sage Publications.

Introna, L.D. 1997. "Privacy and the Computer: Why We Need Privacy in the Information Society," *Metaphilosophy*, Vol. 28, No. 3, pp. 259-275.

King, Gary, Christopher J. L. Murray, Joshua A. Salomon, and Ajay Tandon. 2004. "Enhancing the Validity in Cross Cultural Research," American Political Science Review, Vol. 98, No. 1, pp. 191-207.

King, Gary. 2003. *The Anchoring Vignettes Website*, Available at: http://gking.harvard.edu/vign

LaRose, Robert & Nora Rifon. 2003. *Your Privacy Is Assured—Of Being Invaded: Web Sites With and Without Privacy Seals*. Proceedings of the E-Society 2003 Conference, Lisbon, Portugal: International Association for the Development of the Information Society, May 2003.

Lasch, Christopher. 1995. *The Revolt of the Elites and the Betrayal of Democracy*, New York and London: W. W. Norton & Company.

Lyon, David (Ed.). 2003. Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination. New York: Routledge.

Margulis, Stephen T. 2003. "Privacy as a Social Issue and Behavioural Concept" and "On the Status and Contribution of Westin's and Altman's Theories of Privacy," *Journal of Social Issues*, Vol. 59, No. 2, pp. 243-262 and 411-430.

Marx, Gary T. 2006. "Varieties of Personal Information as Influences on Attitudes towards Surveillance", in Kevin D. Haggerty and Richard V. Ericson (Eds.) *The New Politics of Surveillance and Visibility.* Toronto: University of Toronto Press, pp. 79-110.

Marx, Gary. 2001. "Murky Conceptual Waters: The Public and the Private," *Ethics and Information Technology,* Vol. 3, No. 3, pp. 152-169.

Milberg, Sandra J., H. Jeff Smith and Sandra J. Burke. 2000. "Information Privacy: Corporate Management and National Regulation." *Organization Science*, Vol. 11, No. 1, pp. 35-57.

Mladen, Caryn. 2003. "Privacy in Canada," in *International Report on Privacy for Electronic Government*, funded by the Ministry of Public Management, Home Affairs, Posts and Telecommunications of Japan, pp. 253-314, Available at: www.joi.ito.com/joiwiki/PrivacyReport

MORI. 2003. *Is It Safe to Combine Methodologies in Survey Research?* London: MORI research Methods Unit.

Osborne, Thomas and Nikolas Rose. 1999. "Do Social Science Create Phenomena? The Example of Public Opinion Research," *British Journal of Sociology*, Vol. 50, No. 3, pp. 367-396.

Packard, Vance Oakley. 1972. *A Nation of Strangers.* New York: McKay.

Privacy and Human Rights. 2003. *An International Survey of Privacy Laws and Developments.* Electronic Privacy Information Center and Privacy International. Available at: http://www.privacyinternational.org/survey/phr2003/

Public Policy Forum. 2003. *Biometrics: Implications and Applications for Citizenship and Immigration*, Report on a Forum hosted by Citizenship and Immigration Canada, Ottawa.

Putnam, Robert D. 2000. *Bowling Alone: The Collapse and Revival of American Community*, New York: Simon and Schuster.

Raab, Charles D. 1999. "From Balancing to Steering: New Directions for Data Protection," in Colin Bennett and Rebecca Grant (eds.) *Visions of Privacy. Policy Choices for the Digital Age*, Toronto, Buffalo and London: University of Toronto Press.

Regan, Priscilla M. 1995. *Legislating Privacy. Technology, Social Values and Public Policy*, Chapel Hill & London.

Riesman, David. 1950. *The Lonely Crowd: A Study of the Changing American Character*, New Haven: Yale University Press.

Schwartz, Barry. 1968. "The Sociology of Privacy," *American Journal of Sociology*, Vol. 73, No. 6, pp. 741-752.

Sennett, Richard. 1977. *The Fall of Public Man*, Cambridge: Cambridge University Press.

Solove, Daniel. 2002. "Conceptualizing Privacy," *California Law Review*, Vol. 90.

Taipale, K. A. 2003. “Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data,” *Science and Technology Review*, December.

Westin, Alan F. 2003. “Social and Political Dimensions of Privacy,” *Journal of Social Issues*, Vol. 59, No. 2, pp. 431-453.

Westin, Alan F. 1967. *Privacy and Freedom*, New York: Atheneum.

Worcester, Robert in collaboration with Marta Lagos and Miguel Basanez. 2000. *Problems and Progress in Cross-National Studies: Lessons Learned the Hard Way*, MORI, Available at: www.mori.com

World Economic Forum. 2005-2006. The Global Competitiveness Report. Available at: http://www.internetworldstats.com

World Values Survey. Available at: http://www.worldvaluessurvey.org/