# Appendix A
# Overview of Public Opinion Research Regarding Privacy

**Elia Zureik**

**To be Discussed During the 3 March, 2004 Workshop**

**Comments are welcome. Send to: zureike@post.queensu.ca**

## Introduction

The paper is a sequel to the Concept Paper that was sent to you two weeks ago. The purpose of this paper is to provide an overview of public opinion data related to various aspects of privacy - whether measured directly or indirectly. The exercise is useful to familiarize one with the sorts of questions asked in survey research (and any shortcomings thereof), including the nature and extent of privacy coverage/ operationalization in questionnaire items. As expected, publicly available cross-national data on privacy are not extensive. Nevertheless, there is enough information, particularly about Western countries, to give us a sense of the scope of interest in cross-national privacy issues. By its very nature, this exercise will consist of brief summaries and listing of major sources on public opinion data, with their URL where applicable. I summarize in almost point form the findings of surveys that are primarily national in scope. This will be useful to inform our own survey design and eventually situate our findings in the context of other surveys. Needless to say, most of the sources listed below are available in the public domain. There is no doubt that there are other unpublished privacy studies beyond my reach that are carried out by commercial polling organizations in behalf of their clients.

## Who Studies Privacy Attitudes?

Popular, commercial and academic interest in the study of privacy has increased significantly in the last two decades. This is due to the pervasive use of surveillance technology in commercial and social life, and the impact of political developments at the national and international arenas. Gauging public attitudes to privacy has increased as a function of various (pending and enacted) legislations with clear implications for privacy, and the need by various governments, international organizations, and global businesses to harmonize privacy legislations. I list below what I consider to be some of the key studies of public opinion surveys on privacy. A thorough, more systematic summary of these findings will appear in a future report. Sources for public opinion and attitudinal studies of privacy are divided according to the following categories: (1) advocacy groups, government agencies, think tanks and research centers; (2) commercial polling organizations; (3) other quantitative studies; and (4) qualitative research.

## Advocacy Groups, Government Agencies, Think Tanks and Research Centres

**The Electronic Privacy Information Center** (EPIC), a privacy advocacy group, posted (www.epic.org/privacy/) a compilation of American public opinion surveys of privacy which extended from the early 1990s to 2002. In addition to listing data and press releases by major commercial polling organizations, EPIC provided data from media outlets, think tanks and research centers. EPIC cooperates with Privacy International in publishing the annual report *Privacy and Human Rights 2003. An International Survey of Privacy Laws and Developments*, (http://www.privacyinternational.org/survey/phr2003/).

As an advocacy group, Privacy International's mission is to expose what they see as government and private sector violations of citizen privacy. While they do not carry out polling as such, the web site provides links to relevant privacy studies. Among research centres in the United States, the Pew Charitable Trust published a detailed study in 2000 titled *Trust and Privacy Online: Why Americans Want to Rewrite the Rules* (www.pewinternet.org/). Similarly, The Merkle Foundation (www.markle.org) prepared *Toward a Framework for Internet Accountability* in which attitudes to privacy were examined. The survey was carried out by the public opinion firm Greenberg Quinlan Research (www.greenbergresearch.com). The Annenberg Public Policy Centre of the University of Pennsylvania sponsored a study by Joseph Turow, *Americans and Online Privacy: The System is Broken,* 2003 (www.appcpen.org). Consumers International prepared a study with financial support from the European Commission titled *An International Comparative Study of Consumer Privacy on the Internet*, 2001 (www.consumersinternational.org/). The Opinion Research Corporation (ORC) under the direction of Al Westin published *Public Attitudes Toward the Uses of Biometric Identification Technologies by Government and the Private Sector*, 2001; 2002. Privacy was examined in the context of the use of biometrics in a national ID card in the United States. A report on privacy practices by web sites was prepared by Ernest and Young for the Freedom and Progress Foundation (www.fpf.org). The report was authored by William F. Adkinson, Jr., Jeffrey A. Eisenbach and Thomas M. Leonard, *Privacy Online: A Report on the Information Practices and Policies of Commercial Web Sites*, Washington, DC, 2002. Consumer WebWatch commissioned Princeton Research Associates to conduct a privacy study that focuses on online privacy, which resulted in *A Matter of Trust: What Users Want from Web Sites. Results of a National Survey of Internet Users*, 2002. The Internet Privacy Centre at Georgetown University published few years back *The Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission*, 1999 (www.msnb.edu/faculty/culnanm/gippshome.html). Based on a survey that was carried out by ORC International, The Department of Justice in the U.S. published *Public Attitudes toward Uses of Criminal History Information. A Privacy, Technology and Criminal Justice Information Project*, Washington, DC, 2002. The American Association of Collegiate Registrars and Admissions Officers, Washington, DC issued *Identifying when Technology Logging and Monitoring for Increased Security End and Violations of Personal Privacy and Student Records Begin*, 2001 (www.aacrao.org). The Centre for Communication Policy at University of California in Los Angeles published Harlan Lebo's *Surveying the Digital Future*, 2000 (www.ccp.ucla.edu) in which privacy issues were touched upon in the context of the internet and the workplace.

**In Canada**, Statistics Canada used its General Social Survey 2000 to explore the use of the Internet and its social impact on Canadians (see Heather Dryburgh, *Changing our Ways Why and How Canadians Use the Internet*, 2001). It addressed the issue of privacy and online security only tangentially. For example, it noted that 43% of those sampled indicated that they were concerned about security during financial transactions on the internet, while 17% had no such concerns. In line with other findings, only 5% of those who use the internet reported experiencing problems associated with security. Forty per sent expressed concern about privacy issues, such as when their e-mail is read by others or their web use is monitored.

**The province of Alberta** commissioned two privacy surveys in 2000 and 2003: *Albertans' Awareness of and Views on Privacy*, 2000; and *Stakeholders Survey*. *Report Highlight, 2003* (www.oipc.ab.ca/Publications).

In the **UK**, the MORI social research institute undertook a public opinion survey for the Department of Constitutional Affairs which resulted in *Privacy and Data-Sharing. Survey of Public Awareness and Perceptions*, London: 2003. The European Commission posted the results of a web-based survey of privacy attitudes in EU member countries, *Your Views on Data Protection, Questionnaire for the Implementation of the Data Protection Directive (95/46/EC)*, 2002 (www.europa.eu.int/yourvoice/results/204/index_en.htm). Both of these studies will be summarized in subsequent section of the paper.

**Privacy in the workplace** continues to receive special attention from various stake holders. In its annual survey of workplace monitoring and surveillance, the American Management Association (AMA) (http://www.amanet.org) discovered that 77% of major U.S. firms engage in "total monitoring", and if Internet monitoring is included the proportion of firms experiencing total monitoring rises to 82% (2001). Total monitoring refers to the recording and reviewing of telephone conversations, voice mail messages, computer files, and e-mail messages, in addition to monitoring of Internet connections, and video recording of employee job performance. Other forms of monitoring include time spent on making telephone calls, the number of calls made, time logged on and off the computer, keystroke count, and video surveillance. The storage and review of employee computer files rose from 13.7% in 1997 to 36% in 2001, and storage and review of e-mail messages climbed likewise from 14.9% to 46.5% for the same period. Monitoring of Internet connection increased from 54.1% to 62.8% between 2000 and 2001, when the same question was asked over the two time periods. More than half of the responding firms use blocking software to prevent employee access to the Internet, and 40% apply blocking software to specific web sites, which is up from 29% a year earlier. According to the AMA, companies resort to the above-mentioned monitoring and surveillance technologies due to legal compliance as required from regulated industries, legal liability, performance review of workers, productivity measures, and security concerns. Close to 90% of the firms that engage in monitoring and surveillance inform their employee of the practice (*AMA Survey. Workplace Monitoring and Surveillance of Key Findings,* 2001).

In contrast to the AMA study, the Privacy Foundation data, which were based on self-reporting, discovered that only one-third of on-line workers in the U.S. had their Internet and e-mail monitored by employers. In addition to the self-reporting feature of the study, the AMA and the Privacy Foundation (www.privacyfoundation.org) surveys differed in regard to the wording of the questions. The AMA referred to spot monitoring, while the Privacy Foundation asked about "continuous monitoring". According to Schulman, the author of the study, continuous monitoring is a "dragnet-style 'sweep', a blanket, *suspicionless* [italics in origin] search that carries with it grave privacy concerns" (Schulman, *The Extent of Systematic Monitoring of Employee E-Mail and Internet Use*, Privacy Foundation, 2001:2.

In the United States, 35% of an estimated 40 million on-line workers are monitored, and by extrapolation 27% of 100 million workers worldwide are monitored. The Privacy Foundation estimates that there are 4 million on-line workers in Canada, which brings the total on-line workforce in North America to 44 million. What is interesting about this study is their conclusion that the driving force behind monitoring is the low cost of the software, particularly for large companies. When dividing the revenues from the sale of employee-monitoring software by the number of online employees, it is estimated that employers incur a cost of between $4 and $5 per employee annually.

A survey of human resources managers, carried out by the Center for Internet Studies and Websense Inc., a large manufacturer of employee monitoring software, found out that 56% of employees make inappropriate use of the Internet, while one-third of those surveyed indicated that they are not concerned about Internet use in the workplace. More than 80% of companies in the study, which ranged in size from a high of 10 000 to a low of six employees, mentioned providing employees with written Internet use policies. One in five of the companies using monitoring software, used it to block pornography, 8.9% to block access to hate groups, 6.3% gambling, and 4.5% gambling (Fordham 2000).

### Commercial Polling Organizations

For our purpose, of the various **commercial polling organizations** which carry out research in the privacy area, I list in summary form the activities of five organizations: HarrisInteractive, Gallup Organization and Roper Centre (United States), MORI and ICM (Britain), Ipsos and EKOS (Canada), and others (Australia, Hong Kong).

### United States

**HarrisInteractive** conducted a landmark study for IBM on internationalattitudes to privacy that was published as *IBM Multi-National Consumer Privacy Survey*, 1999. As Priscilla Regan (2003) points out, this article showed national differences in the regulation of privacy. With the lead statement, "Privacy means different things to different people," Harris, with participation by Westin (Poll # 17, 2003, available at www.harrisinteractive.com/harris_poll/) asked American national samples in 1994, 2001, and 2003 to rank the following in importance using a five-point Likert scale:

(1) Not being disturbed at home (**territorial privacy**)
(2) Not being monitored at work (**bodily privacy**)
**(3)** Being in control of who can get information about you (**informational privacy)**
(4) Having someone watch you or listen to you without your permission (**privacy of communication**)
(5) Controlling what information is collected about you (**informational privacy**)
(6) Being able to share confidential matters with someone you trust (**privacy of communication**)
(7) Being able to go around in public without always being identified (**territorial privacy**)
(8) Having individuals in social and work settings not ask you things that are highly personal (**privacy of communication**)
(9) Being able to have times when you are completely alone, away from anyone else (**territorial privacy**).

It is clear that these items correspond to Westin's four types of privacy pertaining to personal lives that I mentioned earlier (intimacy, solitude, anonymity and reserve). In cooperation with Harris and Associates, Westin (2003) explored what he called the "ideological positions' regarding privacy exchange. By comparing 1995 and 1999 data, he discovered that in both surveys slightly more than 50% of the respondents were classified as "pragmatists" (individuals who were willing to examine policies governing tradeoff of information for personal benefit), and between 20% to 25% were classified as either "unconcerned" (ready to supply information about themselves to business and government with no hesitation) or "fundamentalists" (those who rejected any personal information tradeoffs and insisted on strict regulatory measures to protect privacy). By 2001, the proportion of the unconcerned declined to 8%, the fundamentalist share rose to 34%, and the pragmatists registered 58%. By March 2003, a HarrisInteractive report recorded that the share of the pragmatists extended to 64% of the sample, while privacy fundamentalists stood at 26%, and the unconcerned at 10% (Harris Poll #17, www.harrisinteractive.com/harris_poll/). In a series of reports, HarrisInteractive summarized the results of its public opinion polls with regard to privacy and homeland security, and compared the data for 2001, 2002, and 2003 (Report 14, March 10, 2003). Privacy in the workplace was examined by drawing a web-based sample and conducting the interviews online (Report # 32, July 10, 2002). In a series of public opinion polls, HarrisInteractive assessed the attitudes of Americans to national ID card, use by government of surveillance technologies, abuse of personal consumer information, and physical checks of travelers at border points. Americans endorse the use of national ID cards, special surveillance powers by the government, increased monitoring in the workplace, and increased border checks. These attitudes prevailed even though Americans highlighted the danger posed to their privacy by these technologies. The majority of Americans think that there is excessive use of unsolicited mail on the internet. The proportion of Americans who felt that "consumers lost control over their personal information" increased from 56% in 1999 to 79% in 2002.

Exactly one year before the terrorist attack on the United States, **The Gallup Organization** mounted an extensive survey that dealt with privacy issues: (a) 82% expressed concern about privacy online; (b) 72% of users paid attention to whether confidentiality of personal information is being observed during web surfing; (c) 50% said the government should do more to ensure citizen privacy online, while 41% said it is doing enough; (d) 51% opposed and 41% favoured internet service providers giving the courts access to email logs; (e) two-thirds were concerned about government use of spy software; (e) 60% were concerned about the existence of databases that allow access to public records; (f) 54% were concerned about government's ability to tap into a suspect's files at a home computer; (g) three-quarters expressed concern about corporate websites gathering personal information about consumers; and (f) three-quarters were concerned about internet advertisers marketing information about people (*Poll Analysis*, November 2000, available at www.gallup.com/poll/releases/pr001127b.asp ). Similar concerns were expressed in an online survey that was carried out in June 14-25, 2001. Here the survey went further than the earlier one and examined the level of concern regarding (a) privacy risks affecting the use of credit card information that is given over the internet (82%); (b) companies using personal information of customers for marketing purposes (73%); (c) using "cookies" to track internet usage (71%); (d) monitoring practices by internet service providers of e-mail and web surfing (61%); (e) someone forwarding users' e-mail to a third party without prior agreement (50%); and (f) monitoring use of the internet and e-mail in the workplace (39%). Willingness of e-mail users to part with personal information depended on the type of information in question. The same Gallup survey showed that 11% were willing to divulge social security number, 33% credit card number, 35% home phone, 47% date of birth, 49% street address, 83% work phone, and 78% e-mail address (Poll Analysis, June 28, (www.gallup.com/poll/releases/pr010628.asp?Version=p). Nearly two weeks after the terrorist attack, a Gallup poll explored the attitudes of Americans towards surveillance of Arab Americans. What is significant about the findings is the willingness of Americans surveyed to condone the application of special security measures to monitor Arabs in the United States, at a time when (in another survey for CBS News/New York Times and cited by Gallup) close to half of the American public believes Arabs will be unfairly treated in the United States. Close to 60% of those surveyed by Gallup supported the use of extra security at airports against Arabs in the United States, and the public is split evenly on whether Arabs who are American citizens should be required to carry special identification card. A related finding of Newsweek poll that was carried out on September 13-14, 2001, shows that one-third of Americans endorsed the use of special surveillance technique against Arabs that are similar to those used against the Japanese-Americans during World War II (cited in Poll Analysis 28 September, 2001, www.gallup.com/poll/releases/pr010928.asp?Verision=p). By June, 2002, 30% of Americans favoured making it easier for legal authorities to access private communications of citizens which included e-mail and telephone conversations, and 71% approved the use of national ID cards (Poll Analysis, 11 June, 2002, (www.gallup.com/poll/releases/pr020611b.asp).

Like other polling organizations, **The Roper Centre** reports cite data collected by other polling organizations. For this reason, I will provide an overview of those findings that have not been covered earlier by other polling organizations. In its November/December issue, Roper's magazine *Public Perspective* compiled public opinion data on privacy from several polling organizations (http://www.ropercenter.uconn.edu/ pubper/pdf/pp116b.pdf), and grouped them according to the following themes: policing of privacy, willingness to participate in a program that exchanges personal information for benefits, consumers' feeling about control of personal information, and concerns over personal privacy in general. Roper and other data show that while the concern of the American public regarding personal privacy rose steadily between 1978 and 11 September, 2001, such concern showed significant decline following 11 September, 2001 when the public was willing to forego privacy guarantees for the sake of security and safety. Whereas in 1978, 64% were evenly split between "somewhat concerned" or "very concerned" about threats to privacy, the combined figure rose to 88% leading up to the terrorist attack. However, in an October-November, 2001 poll carried out by International Communications Research and cited by Roper, the combined proportions dropped to 62%. And in August 2003, only 17% said they were more concerned about losing legal and privacy rights than with the threat of terrorism, 49% said they were equally concerned, and one-third were more concerned about safety than privacy (*Public Opinion Matters*, www.oprcnter.uconn.edu). Several other polls that are of interest to us were published in the Roper's *Public Opinion Matters* digest: 54% favour racial profiling at airports (June, 2002); 86% favoured higher investment in Homeland Security infrastructure (February 2002). The latter question was posed in such a way so as to tie spending by Homeland Security to job creation. A final question that originated in a HarrisInteractive survey and carried out in 21-24 September, 2001 asked the following: "Do you believe it is extremely important, very important, somewhat important, not important or not at all important …linking passenger identification to boarding passes and baggage?" 57% said it is extremely important, 34% very important, 6% somewhat important, and the remaining 3% said it either not important or did not know. The debate over national ID cards has a long history that dates back to the 1940s. The following is a summary of polls found in various reports compiled by Roper's *Public Opinion Matters*:

Attitudes of Americans to National ID Cards

| Year | Favour | Oppose | Question Highlight |
|---|---|---|---|
| 1942 | 69% | 25% | everyone should carry national ID |
| 1977 | 65% | 30% | same as above |
| 1980 | 62% | 33% | same as above |
| 1983 | 66% | 31% | same as above |
| 1984 | 53% | 46% | reference to national work ID card |
| 1985 | 57% | 39% | card to be used to control illegal entry |
| 1990 | 43% | 56% | reference to national work ID card |
| 1995 | 52% | 43% | to stop illegal immigrants |
| 1997 | 80% | 18% | for purchasers of firearms/ammunition |
| 2001 | 51% | 42% | each citizen issued national ID card |
| 2002 | 56% | 40% | all adults required to carry national ID |
| 2003 | 35% | 54% | voluntary national ID card |

In tracking down the sources of some of the Roper data, an interesting six-nation survey, sponsored by the Council for Excellence in Government (www.excelgov.org/displayContent.asp?Keyword=ppp041403), showed the following results based on samples of internet users:

| | U.S. | Australia | Canada | Singap. | Spain | U.K. |
|---|---|---|---|---|---|---|
| Easy for criminals to forge a national ID card | 56% | 39% | 39% | 36% | 14% | 42% |
| Could be used by government to monitor people | 24 | 34 | 38 | 26 | 30 | 23 |
| Will make it difficult for those who do not have it to prove identity | 13 | 11 | 9 | 14 | 12 | 18 |
| Other/not sure | 7 | 16 | 14 | 24 | 44 | 17 |

Another question that tapped attitudes to a voluntary national ID card in the five countries showed the following variations:

| | | | | | | |
|---|---|---|---|---|---|---|
| Favour | 38% | 48% | 38% | 56% | 48% | 66% |
| Oppose | 52 | 40 | 43 | 24 | 29 | 21 |
| Not sure | 10 | 12 | 19 | 20 | 23 | 13 |

Americans in the same study were presented with two options regarding the use of national ID card: (a) as a facilitator of transactions with the government; or (b) as a means of keeping track of people; the public was split almost evenly with 47% agreeing with the former and 44% agreeing with the latter option.

### Britain

**MORI,** one of the biggest public opinion firms in Britain, has a knack for preparing research papers dealing with methodological problems facing the polling industry. This is probably due to the reputation of its founder and current president, Peter Worcester, who is also affiliated with the London School of Economics. I am pasting from their web site the relevant questions which were included in their survey 10 days after the terrorist attack on the United States. The survey had these characteristics: MORI interviewed 513 adults aged 18+

- Interviews were conducted by telephone on 21 September, 2001;
- Results are based on all respondents unless otherwise stated;
- Data are weighted to the known population profile;
- An '*' indicates a finding of less than 0.5%, but greater than zero;
- Where percentages do not add up to exactly 100% this may be due to; computer rounding, the exclusion of "don't knows" or to multiple answers;
- Poll conducted by MORI on behalf of News of the World.

There has been talk recently about the government introducing a national identity card that people could carry with them. On balance, do you support or oppose the introduction of a national identity card scheme?

| | % |
|---|---|
| Support | 85 |
| Oppose | 11 |
| Don't know | 4 |

On balance, do you agree or disagree with each of the following statements?

**Q9** "Identity cards have been successful in other countries"

**Q10** "Identity cards infringe personal freedom"

| | Q9 | Q10 |
|---|---|---|
| | % | % |
| Agree | 53 | 22 |
| Disagree | 6 | 72 |
| Don't know/depends | 41 | 6 |

Do you think the introduction of identity cards would be successful or unsuccessful …

**Q11** … in helping the Police tackle crime

**Q12** … in helping prevent terrorist attacks

**Q13** … in identifying those who are in the country illegally

| | Q10 | Q11 | Q12 |
|---|---|---|---|
| | % | % | % |
| Successful | 86 | 60 | 77 |
| Unsuccessful | 10 | 32 | 18 |
| Don't know | 4 | 8 | 5 |

**Q14** I am going to read out a number of pieces of information that might be stored on a national identity card. If the government did introduce a card, please tell me whether you would be willing or not for each of these pieces of information to be stored on it?

| | Willing | Not willing | Don't know |
|---|---|---|---|
| | % | % | % |
| Date of birth | 96 | 3 | 1 |
| Photograph | 97 | 3 | * |
| Eye colour | 92 | 7 | 1 |
| Finger print | 85 | 14 | 1 |
| DNA details | 75 | 21 | 4 |
| Religion | 67 | 31 | 2 |
| Criminal records | 74 | 23 | 3 |

**Q15** As you may know, Osama bin Laden is the suspected terrorist accused of the attacks on the World Trade Centre and the Pentagon. Some of his British supporters have called for a Holy War against the West. Do you think they should or should not be prosecuted for inciting racial hatred?

| | % |
|---|---|
| Should | 69 |
| Should not | 17 |
| Don't know | 14 |

A survey, carried out by MORI between June-July 2003 for the Department of Constitutional Affairs in Britain, attempted something that is relevant to our concerns, that is, examine the level of public awareness, experience and perceptions regarding personal data held on citizens by the government: (a) 64% are unaware what type of data is held on them; (b) 74% don't know how to go about finding what personal information is held on them; (c) 68% don't know how to make a complaint; and (d) 53% don't know what their rights are when it comes to personal information. When asked about what constitutes "personal information", with no less than 30 definitions given, the top six types of personal information included, in descending order, health records, income and tax records, address, police records, family records and DNA. While 64% say they are not informed about the information that is held on them, an equal percentage said that they want to know more. Low level awareness of how personal information in handled by the government, is accompanied with concern about the information (60%). Based on contact with various government departments, 34% were not told why the information that is held on them is needed; 25% whether the information would remain confidential; and 1% of how the information would be stored. These responses refer to a minority of respondents, since 96% did not approach public officials seeking information about themselves.

At a time when there is an intense debate in Britain over the government's proposal to introduce national ID card, an **ICM** poll revealed that only 26% agree that the "government can be trusted to keep our personal information secure," 58% disagree, and the remaining 16% have no opinion. However, similar to Canada and the US, the British survey showed willingness on the part of the majority (72%) to give up some privacy rights in order to fight terrorism. Yet two-thirds of those polled in July 2002 expressed concern that personal information about them is not secure as it travels through e-mail and text messaging. Only one in five is willing to grant local authorities access to telephone or Internet records ("Privacy Fears Revealed," *Guardian*, 7 September 2002, available at www.guardian.co.uk).

**YouGov**, another British polling organization, surveyed the attitudes of the British public in September 2003 to the proposed ID Card in behalf of the conservative newspaper *The Daily Telegraph* (www.YouGov.cm). While there was substantial acceptance of the ID card idea among close to 80% of the public, two-thirds thought that eventually such a card would carry confidential personal information such as health and DNA records. These are types of information that the majority of the public felt should remain confidential and beyond the reach of government. As well, one-half thought that data on the ID card would be divulged to third parties. This supports another finding in the survey which showed that 60% feared abuse by government of the data stored on ID card. Although between 7% and 13% agreed that the police should use the ID card to target racial minorities and “foreign-looking people,” close to 48% felt that the police would actually use the card to target “racial and other minority group,” and 37% said the police would do the same for “foreign-looking people.” An overwhelming majority said the police would use the card to catch known and suspected criminals (82%), welfare fraud (82%), and asylum seekers (75%). The public was in agreement that the police should use the card for such purposes.

British evidence, which relied on a survey of 74 British organizations, shows that 77% of employers visited web sites used by their employees, and 55% monitored the e-mail and Internet use of their employees (Computer Weekly 2000).

## Canada

**EKOS Research**: As I mentioned in the Concept Paper, the 1993 EKOS’s *Privacy Revealed* was one of the early, detailed surveys about attitudes towards privacy in Canada. It is highly innovative, and is worth summarizing its key findings because they shed light on the evolution of Canadian attitudes to privacy. The results, which were based on a sample of 3000 Canadians, revealed that more than 90% of those sampled are generally concerned about privacy issues. Four out of five believe that computers endanger their sense of privacy; 54% express "extreme" concern over the computer's ability to link personal data stored on several computers; and 60% thought that at the time there was less privacy than a decade earlier. These concerns are not necessarily based on personal experience, given that only 18% of those surveyed said that they had experienced serious privacy invasion.

When asked to give examples of "serious invasions" of privacy, only 3% ventured to do so. The category that captured first place was that of crime, followed by disturbance, psychological harassment, information abuse, credit and financial data problems, and finally workplace surveillance. As the report notes, the inability of a larger number of respondents to name privacy violations has to do with the "invisible" nature of privacy problems. What is extraordinary about the EKOS survey is that it foretold of later developments in the privacy field, namely: that (a) knowledgeable people, as well as those who are least informed, tend to manifest the highest level of concern about privacy violations – but obviously with different motivations; (b) the more transparent the rules are, the less concerned individuals are that their privacy would be violated; (c) having a sense of consent and control over the process of information storage and its release makes people feel comfortable that their privacy will not be violated; those who accept the rationales given for privacy protection, and who see benefit in it, tend to be less concerned with privacy issues; and (d) perceptions of the legitimacy of institutions that hold information about citizens are correlated with lower levels of concern that these institutions might violated one's privacy.

In descending order, Canadians give the rank the various dimensions of privacy according to the following: (a) not being watched or listened to (75%); (b) being in control of who has access to information (70%); (c) controlling what information is collected (63%); not being disturbed at home by marketers (42%); and not being monitored at work (36%).

In March 2001, EKOS released a six-volume study, *Rethinking The Information Highway. Security, Convergence and E-Commerce/E-Citizen*. Volume IV, *Privacy, Security and the Internet*, is of interest to us. This is the most comprehensive, publicly available Canadian privacy study that I have seen. It is based on a panel design of more than 5000 respondents, with around half of them interviewed twice over a period of time. The study explored some of the issues raised in previous EKOS surveys that were carried out in 1992 and 1999. In particular, the 2001 study examined what people understood privacy to mean, privacy concerns in terms of type of information in question (credit card number, financial situation, social insurance number, health history, etc.), type of organization seeking personal information (telemarketers, internet service providers, polling companies, telephone companies, etc.), assessment of personal privacy status relative to the past, concern over online privacy, use of a single ID card for identification purposes and multipurpose use, trust in government and private sector organizations in handling personal information (Health Canada, Revenue Canada, a large bank, Canada Post, etc.), extent of familiarity with security and privacy-related technologies (cookies, encryption, public key infrastructure, etc.), perceptions of online security (willingness to give credit card number over the internet), trust and comfort in submitting financial transactions over the internet, and willingness to give fingerprints in order to provide more security for personal information, Following the terrorist attack on the United States, EKOS released in September, 2001 *Security, Sovereignty and Continentalism: Canadian Perspectives on September 11, 2001*. This study, which was conducted in behalf of the Toronto Star, Le Presse, and CBC/SRC, showed that 59% of Canadians "don't mind giving up some of our national sovereignty if it increases the overall sovereignty of North America." Nearly two-thirds of Canadians thought that the events of September 11 would restrict movement across the border between Canada and the US. While 40% of all Canadians disapprove of airport check-in times increasing by one to two hours, among visible minorities it is 58%, and for non-visible minority Canadians the proportion is 38%. Undoubtedly, this is a statistically significant difference, and it underscores suspicion among visible minorities that profiling is primarily aimed at their group.

As the interest in national ID card gathered momentum, we began to see more concentrated reference to issues of technology and privacy. In 2003, Pollara discovered that 73% of Canadians were in favour of a biometrics ID card, and in excess of 80% supported the use of biometrics in passports, airports, government programs, and border crossings, even though the public knew very little about the details of the technology. However, more than one-third of Canadians thought that the use of ID card "goes against Canadian values of freedom and fairness," and more than 50% said it would reduce privacy. The EKOS poll of the same year was more substantial in its scope, although the overall picture that emerges is the same. Only 15% knew what the term biometrics meant. There was greater support to voluntary than mandatory government introduction of the ID card. As I pointed out in the Concept Paper, The survey did offer some contradictory interpretations. For example, 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% agreed with the statement that "there is a serious problem with groups supporting terrorist activity in Canada," and 61% agreed to the statement that "given the potential of terrorism, the Government of Canada should be given special (extraordinary) powers to deal with possible terrorism-related offences." As I will demonstrate in the section on qualitative research, it would have been possible to get at the nuances of such inconsistent responses through the use of open-ended and/or focus group methodology.

**Ipsos-Reid,** the largest polling organization in Canada, is a member of the Ipsos Group, a global polling organization with offices in several countries. The publication *Ipsos-Insight* (www.ipsos-na.com), which among other things tracks internet use starting in 1999, released on 20 January, 2004 *The Face of the Web 2003*, an annual publication that surveys internet use in 13 countries. With a sample of 7100 adults, half of whom (3250) are active internet users, data for 2003 show that Canada has the highest rate of internet use (71%), followed by South Korea (70%), United States (68%), Japan (65%), Germany (60%), United Kingdom (54%), France (43%), urban China (41%), urban Mexico (37%), urban Brazil (21%), urban India (19%), urban South Africa (15%), and urban Russia (10%).

Another international survey of consumer attitudes to privacy covering 4000 respondents in four countries, was released on 12 November, 2003 by the Ipsos office in Washington D.C. The relevant tabular results for our purpose are as follows:

Per Cent Expressing Great Deal/Fair Amount of Concern

| | U.S. | Mexico | Japan | U.K. |
|---|---|---|---|---|
| Information sold to third parties | 83% | 74% | 92% | 56% |
| Information stolen from databases | 79 | 77 | 89 | 57 |
| Transmitting credit card number | 76 | 78 | 86 | 55 |
| Transmitting address/personal info. | 77 | 75 | 82 | 53 |
| Receiving unwanted email | 73 | 66 | 74 | 46 |

On 15 October, 2003, Ipsos-Reid published its comparative report which dealt with American and Canadian attitudes to business relations between the two countries in the context of border security and possible introduction of a national ID card. While 47% of Canadians agree with the government issuing of ID card, and 52% disagree with the proposal, among Americans the corresponding figures are 40% and 59%, respectively. Only 15% of Canadians, compared to 28% of Americans, say that a "better use of technology at the border for security purposes" would have the best chance of improving business relations between the two countries. Among a national sample of 678 credit card users, an Ipsos-Reid survey that was released on 13 July, 2003 discovered that 50% were concerned that online data may be intercepted, 58% expressed security concerns about the databases that store personal information, and 65% expressed confidence that financial institutions would be able to protect the privacy and security of financial transactions. A combined sample of web users (1000) and those interviewed by telephone (1000), reported a drastic increase in the percentage of those concerned about online security - from 18% in 2001 to 32% in 2003. Thirty-five per cent reported in 2003 that they have experienced privacy breach with regard to their personal information given online, twice the number of those who made similar claims in 2001. More than 8 out of every 10 Canadians expressed concern about giving personal information online. The concerns had to do with the safe storage of information in databases, use of credit information by unauthorized people, interception of data transmitted online, authentication of the card-holder's identity by credit companies, and that the sites users visit can access information stored on their personal computers. All of these factors were considered an impediment to furthering business transactions online. Based on a combined sample of 1000 each of web users and telephone interviewees, an April 2003 survey of employees recorded the following:

- Two-thirds agreed that employers have the right to monitor employees' e-mail and internet usage;
- 57% indicated that their workplace has a policy regarding personal use of the internet – up from 33% in 2000;
- While personal use of internet is perceived to lower productivity, some see a work-related benefit derived from it as well;
- Close to 9 out every 10 employees indicated that they have access to the internet at work.

Because of increase in unwanted advertising by telemarketers (from 62% in 1999 to 79% in 2002), a survey conducted in March 2002 revealed that three quarters were unwilling to give personal information to online retailers. Two months after the 11

September, 2001 attack, a survey in November 2001 revealed that although 80% agree to fingerprinting for national ID card, 59% are opposed to random searches by the police. However, 85% think that current threats of terrorism outweigh individual rights and due process of law; 52% believe it is necessary to give up some of the civil liberties in the fight against terrorism; and 38% feel that the Charter of Rights should be respected. The highest percentage of those agreeing to fingerprinting came from Alberta (62%), followed by the Atlantic Provinces (60%), Ontario (56%), British Columbia (55%), Saskatchewan/Manitoba (49%), and Quebec (36%).

On 27 June, 2001, Ipsos-Reid released the results of its 16-country survey which showed that close to three-quarters (72%) of the more than 8000 respondents expressed concern about online credit fraud. This concern resulted in a three-fold recommendation: the need to educate consumers about security of personal information; to have clear disclosure of corporate privacy policies written in a language that is easy to understand; and to stress to consumers that credit companies do have in place mechanisms to protect against fraud and identity theft.

With a sample of 800 office workers drawn from six major Canadian cities, Ipsos-Reid released the following results on 31 May, 2001. More than 9 out of 10 workers concurred that "fast and easy access to information is a critical part of their job." More than 90% said that they collaborate electronically with others in their organization on the same document, and three-quarters rated sharing information with co-workers as important. Yet, in another survey that was released on 26 March, 2001, 60% don't believe that enough is being done to protect online cybercrime, and that online criminals have a lesser chance of being caught compared to real world criminals (72%:18%). A combined sample of 1000 web respondents and 1500 telephone interviewees concluded that 8 out of every 10 respondents shared personal information on the web, 74% relied on the company's reputation for carrying out transactions, and 36% that increase in government involvement will make them more willing to share online information. Of the 18% who said that they experience privacy breaches, 81% said it resulted in unwanted email, and 43% claimed that their personal information was sold to third parties. Online privacy concerns can be seen as early as 2000, when Ipsos-Reid sampled in excess of 1000 web users and additional 1500 telephone interviewees. More than 80% expressed concern about personal information, such as credit card numbers being compromised; three-quarters did not make online purchase because of privacy concerns; 62% were concerned about the safety of the databases in which information is stored; and 51% expressed concern about company verification of credit card users.

## Other Quantitative Research

While **a**dmittedly not based on a representative sample, a multi-country online survey of 9156 internet users in the **EU** countries produced results that are consistent with North American data. The level of awareness regarding data protection in the EU was ranked sufficient/good by 15% of the participants, compared to 81% who said that their level of awareness regarding data protection is insufficient/bad/very bad. Three-quarters did not exercise their privacy right to check the accuracy of personal information that is stored on them in databases (www.europa.eu/yourvoice/results/204/index_en./html).

Results of two privacy surveys are posted on the web site of the **Hong Kong** Privacy Commissioner's Office (http://www.pco.org.hk/). The first survey was carried out in 2000 and consisted of 1600 adults who were interviewed by telephone, in addition to a postal, self-administered questionnaire that was returned by 485 organizations representing 23 sectors. Privacy received a score of 7.6 out of 10 in terms of its importance to the public, thus placing it in the top three public policy concerns after air pollution and unemployment. Examples of privacy invasion included intercepting personal telephone calls during working hours, employers accessing employee e-mail, using video cameras in eating places at work, tracking by employers of employee web site visits, and the placing of video cameras at the entrance to the workplace. When asked to rate various types of privacy issues, financial loss due to interception of credit card information (84%) came first, followed by misuse of personal information by third parties (72%),  insufficient knowledge about vendors (54%), and telemarketing (39%). When it came to participating organizations, the Hong Kong study compared data going back to 1997, 1998, 1999, and 2000 to show that there was a progressive increase in awareness on the part of organizations to comply with privacy standards, the way data is managed, relationship with customers and employees, and to ensure the security of data records. The surveillance tool that is used most frequently by organizations was CCTV (48%), followed by computer monitoring (28%), web-browsing (23%), phone tapping (23%), and e-mail tracking (21%).

The second Hong Kong study was carried out in 2002 and focused on young people between 12-34 years of age. On a scale from 0 to 10, respondents were asked to rate 20 items with regard to privacy concerns. At the top of the list respondents placed ID card numbers, followed by personal address, telephone number, financial situation, medical record, employment record, sexual orientation, etc. One's religion was ranked at the bottom of the list in terms of privacy. It is interesting to note that the level of concern about privacy regarding ID card number, home address, and telephone number rose with increase in age.

In **Australia**, the Federal Privacy Office commissioned a national survey in May 2001 of 1524 respondents to assess community "attitudes towards the protection of personal information and awareness levels of current privacy laws." http://privacy.gov.au/publications/rcommunity.pdf). This is part of three attitudinal studies of privacy in Australia, the other two are *Privacy and Business*, July 2001 (http://privacy.gov.au/publications/rbusiness.pdf), which surveyed the attitudes of the business community to privacy, and *Privacy and Government*, July 2001 (http://privacy.gov.au/publications/rgovernment.pdf), whose focus was the attitudes of managers responsible for handling personal information and officers responsible for facilitating compliance with privacy legislation.

Our overview of the Australian publications focuses on the study of community attitudes to privacy. It is interesting to note that only 20% of those contacted (7469) agreed to participate, 66% refused outright, and the remaining 14% terminated the interview while it was in progress. There is a lesson to be learned here. It could very well be that respondents saw the mere providing of answers to a privacy questionnaire is itself an invasion of privacy. The study was launched after the December 2000 Amendment of the Privacy Act which became law and extended the 1988 Federal Privacy Act to the private sector. In point form, the main results are as follows:

- Proactive respondents concerned about furthering privacy rights tended to be older groups, have higher income, and more educated;

- Knowledge about privacy rights was positively correlated with assertiveness about privacy issues;
- Younger people, and those with lower education, were least assertive with regard to privacy rights;
- In descending order, people felt less inclined to divulge financial information bout themselves, give details about their income, and home address;
- More than 90% rejected the sharing of personal information with third parties or in using it for reasons other than for which the information was originally collected;
- Internet retailers were perceived to be the least trustworthy group regarding protection of personal information;
- 4 out of 10 were prepared to trade personal information for more efficient and personalized service. This was particularly the case among young people and those with high income;
- Although there was convergence between low and high income people in their reluctance to divulge personal information, the rationales were different: for the former it is because of fear and lack of knowledge, while for the letter it is because of privacy rights awareness;
- More than half of the respondents knew very little or nothing at all about privacy rights, while two-thirds of the population scored less than 50 on a possible 100-point knowledge scale;
- Three-quarters condoned data matching across government departments in order to reduce fraud; 81% agreed to the monitoring of health records through the use of unique health identification number; and 55% were willing to grant the police access to their personal information in order to solve crime. If the latter figure indicates lower level of trust in the police, the previous numbers, showing the majority population acceding to the monitoring of their personal information, reflect lack of knowledge on the part of the public of what this entails. Here is how the report described the situation:

  > While these results may indicate lower levels of trust in the police, they may also be explained by findings in the qualitative research which suggests that most people are unaware of the deeper privacy issues surrounding the allocation of unique numbers and data matching. However, as demonstrated in the focus groups, the more they learn about the issues (through knowledgeable group member), the more they began to heavily qualify their acceptance of the one-number concept, or to reject it altogether (p. 6).

  - Finally, in line with results from other surveys, more than 90% of Australians surveyed agreed that the tracking of internet users without their prior knowledge constitutes an invasion of privacy.

## Qualitative Studies

It would be wrong to dismiss small scale quantitative and qualitative studies on account of their limited generalizability. The literature on privacy and monitoring is rich with small scale quantitative surveys and qualitative ethnographic studies, including studies that utilize focus groups. At times researchers have adopted a combined qualitative-quantitative approach. The latter in particular has been useful in explaining what lies behind "surface" opinion expressed in large-scale survey research where close-ended questions dominate. A prototype of the combined approach is the exploratory study by Starr Roxanne Hiltz, Hyo-Joo Han and Vladimir Briller, "Public Attitudes towards a National Identity 'Smart Card': Privacy and Security Concerns," Proceedings of the 36th Hawaii International Conference on System Sciences, *IEE Computer Society*, 2002.

It is worth elaborating on the study by Starr and colleagues, because it deals effectively with the nuances surrounding public reaction to complicated issues such as privacy. As we have seen in the above summaries, a typical finding in privacy research shows the public to be highly supportive of government measures to curtail privacy and civil rights in order to protect national security in the face of terrorism. In the quantitative portion of the Starr study, two-thirds of the sample thought the use of a national ID card to be excellent/good idea. Yet, one-third thought it was a bad idea. When factor-analyzed, several questions loaded on a monitoring factor that related government activities to privacy concerns. Moreover, there was a significant correlation between support for a national ID card and the monitoring factor, which included other government monitoring activities (such as submitting DNA, wiretapping of phone lines, tapping of cellular phone conversations, creating profiles of people from unfriendly countries, and the setting up of databases continuing information on the activities of various groups).

The semi-structured interviews revealed nuanced opinions and "mixed feeling", but more importantly it showed lack of knowledge about the monitoring technology - the proposed national ID "smart" card in this case. People were prepared to accept government monitoring up to a point, more so in certain areas than others. For example, significantly fewer people were willing to include DNA details, medical history, and religion on their national ID card, than those willing to submit to an eye scan, fingerprinting or provide a photograph or date of birth on the card.

In general qualitative research has the added advantage of capturing agency's reactions to surveillance and monitoring practices such as in the workplace and other organizational contexts. It should also be pointed out that small size surveys enable researchers to construct, with the aid of experimental designs, appropriate comparisons between control and non-control groups, things that are difficult to achieve in natural settings.

Very few of the mass administered questions that were referred to above were either open-ended or dealt with means and mechanisms used by people to counter surveillance. Historical or philosophical dimensions of privacy are usually left out of such surveys. For example, it would be interesting to examine the meaning of privacy in East European countries, such as in Hungary and Poland which are part of our cross-national samples, as a result of their experience with the secret police during Soviet hegemony over Eastern Europe.

It is not my intention to review qualitative and small scale quantitative studies here, but to list them according to their type of focus on privacy. Complementing our international, quantitative survey will be a series of qualitative studies carried out on focus groups in order to assist us in developing the survey instrument and in going behind close-ended items.

It is possible to group the qualitative and small scale studies into the following:

- Importance of privacy for psychological well-being and self-worth of individuals;
- Psychological research which focuses on the relationship between surveillance (in particular in the workplace) and job satisfaction, quality of worklife, productivity, and ergonomic factors;
- Relationship between monitoring, supervisory feedback and employee job satisfaction;
- Worker attitudes to monitoring (including resistance) as a function of fair practices at work (procedural and distributive justice issues);
- Attitudes to surveillance in terms of occupational characteristics (office workers, manual workers, service workers, management vs. front-line workers, etc.);
- Due to the emergence of call centres as important component of the labour market, researchers have focused on the working conditions of call centers, with special reference to surveillance and monitoring. This mushrooming research has produced contradictory findings on how to measure surveillance and resistance to it;
- Legal research on monitoring, while it does not involve survey research as such, is expanding tremendously to cover areas of workplace surveillance, genetic testing, biometrics, and CCTV use. A sample of recent legal writings on electronic privacy are the: Robert Thornburg, “Face Recognition Technology: The Potential Orwellian Implications and Constitutionality of Current Uses Under the Fourth Amendment,” *Journal of Computer and Informational Law*, Vol. XX, 2002, pp. 321-346; A. Michael Froomkin, “The Death of Privacy,” *Stanford Law Review*, Vol. 52, No. 2, 2000, 1461-1543.; Daniel J. Solove, “Access and Aggregation: Public Records, Privacy and the Constitution,” *Minnesota Law Review*, Vol. 86, 2002, pp. 1137-1218;Michael Geist, *Computer and E-mail Workplace Surveillance in Canada: The Shift from Reasonable Expectation of Privacy to Reasonable Surveillance*, prepared for the Canadian Judicial Council, May 2002; and Jeremy deBeer, “Employee Privacy; The Need for Comprehensive Protection,” *Saskatchewan Law Review*, Vol. 66, No. 2, 2003, pp. 383-418.

Concluding Remarks:

The above overview 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 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 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.