Globalization of Personal Data Project – International Survey
Findings from the Pre-Survey Focus Groups

Submitted to:

Professor Elia Zureik
Department of Sociology
Queen's University

Barcelona., January 2005

Table of Contents

Introduction

EKOS Research Associates was hired by Queen's University to conduct a series of focus groups in support of the Social Sciences and Humanities Research Council-funded Globalization of Personal Data (GPD) Project.

The GPD Project is an 11-country study of privacy attitudes, involving both quantitative and qualitative research.

The first phase of the project involved a series of preliminary focus groups in advance of commencing the quantitative phase. The main objectives of the pre-focus groups were to provide the research team with qualitative findings in relation to understanding how individuals view the study's areas of research. The findings from this qualitative phase were designed to help shed light on the issues and how they are perceived, with a view to helping frame the questions for the actual survey.

Working with Queen's University, EKOS designed the moderator's guide to address a range of study issues. The moderator's guide encompassed both common and specific issues. Common issues were posed to all participant types, while the specific issues were tailored to the different types (e.g., questions for workers). Where time permitted, some of the specific questions were asked to other groups where relevant (e.g., all travellers are also citizens). All research material was reviewed by the Ethics Review Board at Queen's University prior to conducting the focus groups.

For the Spanish research, EKOS (via Ipsos North America) contacted Ipsos Spain, who recruited, conducted and analysed the 2 focus groups held in Barcelona on the month of January 2005. This is the document that reproduces research's main findings related to privacy in Spain.

It should be borne in mind when reading this report that these findings are drawn exclusively from qualitative research. While every effort is made to balance various demographic characteristics when recruiting participants, these groups (and therefore the findings drawn from them) may not be said to be representative of the larger population as a whole.

Research Methodology

The research findings are based on the following:
In total, two focus groups were conducted during the week of January 25th, 2005.
Focus groups were held in Barcelona.
The groups lasted approximately two hours and were held in dedicated facilities to allow for viewing by clients and audiotaping.
A total of 10 individuals were recruited for each of the focus groups. In total, the focus groups involved the participation of 20 individuals.
Focus group participants were divided into four types: workers, travelers, consumers and citizens within two groups.

DETAILS OF THE FOCUS GROUP	
➢ Number of Focus Groups:	2
➢ Sample Size per Group:	N=10
➢ Sample Target:	Group 1: **Workers'** (work full-time/35+ hours per week) **Travelers'** (traveled by air at least 2 times in the past year) Group 2: **Citizens'** (citizen of country or landed immigrant, and must have contacted local, state, or national government for information in the past year) **Consumers'** (have purchased (or at least have thought of purchasing) a product or service over the Internet in the past year, and are primarily responsible for household's shopping needs)
➢ Other Group Composition Characteristics:	❖ Each group should consist of an equal distribution of males and females. ❖ Each group should generally contain a range of people in age, education, income, and household categories.
➢ Length of Focus Groups:	2 hours each

Key Findings

Perceptions and Experiences with Privacy Issues

At the beginning of the group, participants were required to answer a written questionnaire with the instruction: "write down the first thing that comes to your mind when you think of *privacy and safety*". For participants, privacy and safety have different meanings:

- **Privacy** is associated with respect, intimacy, confidentiality.

It is a very subjective concept and admits being self-controlled: each one chooses the limit of one's own privacy. It is **personal,** one's own, it belongs to each one.

In the mixed citizens/ consumers group, privacy is claimed as a **right. Their attitude was more inconformist.**

The mixed workers/ travelers group makes a distinction between:

▪ *Economic-professional privacy*, related to economic and personal data that have to do with curriculum and work place. The lack of control over one's own banking and financial-tax data generates high levels of worry and fear. There is a feeling that this type of data, which should be absolutely confidential, is actually available for anyone to see.

"…you don't dare get into Internet and leave your data because you haven't a clue where they go to or who's going to look at them…"

▪ *Personal privacy* is related to everyday life and one's own family circle. Information is about health, religion and sexual condition. In that terrain, participants require and demand **respect** and legal protection.

"…some personal data are required on income tax statements, they ask you those questions and you're obliged to answer...and I don't think that is right"

"…use of certain information like homosexuality violates all existing privacy rights …"

- **Safety** is associated with tranquility but there is, nonetheless, a complaint: participants feel the need to increase control mechanisms in order to protect their safety from advancing technology and growth of the databases market containing personal information. In addition we must say that the concept of security is not understand as national security.

Here are some of the control mechanisms developed by participants:

. Destruction of all papers containing personal and/or tax information, such as address, telephone number, etc.

"… I break everything into little bits so that nobody can see it …"

. Filters in Internet to prevent entering into Web pages that could mean trouble.

. Refusing to provide private information to obtain invoices even at the risk of not getting them.

"…they even asked my telephone number for a mere gas bill, so in the end I left without the bill…"

We see that privacy and safety are closely connected because the only way of keeping and safeguarding privacy is by maintaining high safety levels.

It is important to bear in mind the overall impression of absolute **control** held by: the police, the state and private companies. This generates:

- Rage and impotence *"…they've got you on file and you can't kick up a fuss or even open your mouth …"*
  "…I feel like tearing up all the cards and the ID, and everything …"

- Fear *"…and the things they don't tell us!...I'm sure they control us in things we don't even know about. I destroy all the papers so that nobody can get hold of my data …"*

Experiences:

- "I asked in the petrol station for a bill and they told me I had to give my personal data, when they have the obligation to give it to me "
- " My son is autistic and I remember I was looking in Internet in the Web of the Generalitat for some information and two days after my e-mail was full of information of different associations I never heard about"
- " I arrived at home and I was looking my mailbox when I found a sado catalogue

Expectations regarding privacy issues in the future

There is awareness of constant and powerful technological progress and increased growth of the databases market containing personal information; this means that everything related to privacy will be severely threatened and that therefore, in order to preserve that privacy, further safety measures must be taken.
This type of fantasies appears in the imagery:

. implanting microchips that will enable knowing everything about any given person.

. Digital reading machines

"*…you'll put a finger into a little machine and all your life will come out …*"

. Cards containing all banking transactions carried out during one's whole life

. Cards containing FULL information about a given person: banking, tax, health-related data…

"… police will stop you and say that you haven't paid for some trousers you got in Zara…"
"…with a little card they will be able to know what diseases you've had, how much money you have and where you live …"

Beneficiaries of all this attack on privacy are and will be private enterprises, multinational companies like Coca Cola, McDonalds and such, which manage and control the worldwide economy. All this translates into the greatest exponent of control: **power.** This power will encompass both the economic-financial sector and political power. Thus, citizens will be left without an option to choose ANYTHING. Everything, even political management, will be under the control of the big multinational companies. And at the bottom of all this, and fuelling all this power, is **money.** Highlight that companies also use the mechanism of fear and the government to increases a way of control.

Privacy Technologies and Legislation

Participants are aware of the need for current technologies. Internet has turned into an indispensable tool for the development of countless activities: banking transactions, purchases, etc… Although it entails a speed/time-saving/efficacy benefit, it may also contribute to this "*spread*" of information that is an onslaught against privacy, allowing any part of private life to become public, thus jeopardizing safety. There are two attitudes in front of the control that technologies exercises: a negative one who thinks that is just another way of being controlled and the other one whom feels that the benefits are balanced with the inconvenient.
As to legislation, there is basic ignorance regarding data-protection laws. These laws presumably do exist, but:

- There is a total lack of information. Being informed requires consulting an individual/ private lawyer.

- There is no proactive attitude in seeking such legal information. Only in the face of a very serious problem is information sought for and required.

Besides, all this generates disillusion-disappointment. There is a feeling that, in the face of a serious problem due to information-leakage, the only solution is to report it to the police, a court of law, etc. The current situation of legal actions in Spain (slowness, bureaucracy, inefficiency) generates the suspicion that such a denunciation would end up in a long, complicated legal process with a likely negative outcome.
Thus, participants feel alone in the world, defenseless, totally unprotected by data-protection laws and with no rights to privacy.

Privacy Issues Specific to Workers

When asked if big companies control their employees' activities, respondents showed some degree of awareness that companies do in fact exert some kind of control, especially in what concerns telephone calls and visiting Internet pages.
None of the respondents who were interviewed were conscious of being controlled by the company they worked for.

In any case, the control a firm has over its employees is not viewed as an invasion of privacy because it's accepted that companies have a right to control their employees during work hours. These control measures help to draw the line in a situation of mutual trust, and the company is entitled to make sure that employees make proper use and do not abuse the facilities offered, during work hours.
Concerning the issue of what is/ isn't personal in work environments, respondents are aware that companies require some personal data, but are confident that it won't spread them around or misuse them; if it should happen, it would mean stepping over limit and trespassing on privacy.
On the other hand, respondents coincide in that individuals draw their own limits, depending on how much of their privacy they wish to disclose.
The idea of setting up cameras in companies was generally accepted; it doesn't bother them, as long as they are duly notified.

Privacy Issues Specific to Travelers

When addressing the issue of travel-related privacy, and maybe due to recent events and the current situation of "fear", people are willing to submit to established control because it is accepted as a safety measure. It doesn't prevent feeling a violation of privacy, or humiliation, but is viewed as protection against a greater evil.
The measures recently adopted by the USA generate an attitude of understanding among respondents, they accept exchange of information; the only issues they feel slightly uneasy about are the use given to data and the fact of not knowing who is involved in that transfer of information.
In any case, once again the idea emerges that anybody who is informed is free to choose. It is understood that one's power in the face of invasion of privacy lies in the knowledge and information available, in order to set limits or at least to know what one is up against.
Experiences:

- In the airport of Israel naked in front of everyone.
- In the airport of USA being interrogated for seven hours
- The fact that for traveling to USA one haves to have a electronic passport which contains a microchip with unknown information

Privacy Issues Specific to Consumers

Knowledge about the Travel Club program is precarious; those who own the card are vague when they have to define the program and explain its uses or how it works:
"It's for gas",
"For everything",
"Points are allotted".

Discourse is limited to program "benefits":
"They give you points for free trips".

When it was suggested that this type of program could sell its user's purchasing behavior, respondents verbally expressed they didn't know this; even so, they weren't

surprised and seemed to view it as an accepted thing (although they were not fully aware).
Within the group, only two members (citizens segment) expressed outrage by what they consider is an invasion of privacy and improper use of data whose disclosure they don't remember having consented to.
When addressing the purchase-through-Internet issue, those respondents who have actually used this system value it because it's a convenient, practical and sometimes cheaper way of buying. Although no problems were reported, buying over the Internet causes certain insecurity; this is due to not knowing who will have access to the registration data, plus the widespread notion of the vulnerability of the Web's safety mechanisms.
"A hacker could get in and get a look at all my data"
"There are Web pages that teach you how to commit piracy on PCs"

There is complete unawareness about safety laws in Web pages, all respondents admitted they hadn't read the information available, that's why they don't know if protection measures are adequate or not.
"It's very long",
"It's done on purpose so that you won't read it".

Privacy Issues Specific to Citizens

People are used to seeing safety cameras in ATMs, in subways or for traffic.
They are viewed as cameras whose purpose is to dissuade from committing any kind of felony, with somebody on a 24-hour-watch observing surveillance videos, all of which serves to tranquilize pedestrians. Some respondents are skeptical, they don't believe in the camera's dissuasive powers and doubt that there is somebody actually watching the videos. In any case, as long as they're not installed inside homes, cameras were positively valued, with the exception of one respondent (citizen) who showed concern about where to draw the line.
When the London/Canada issue was brought up, reactions once again revealed skepticism about its real capacity as a surveillance system because sooner or later they're bound to find a way of fooling it.
The hint that Barcelona could adopt this strategy generated different opinions: it is a known fact that there are cameras installed in certain points of Barcelona and this is not viewed negatively. The issue of installing more cameras also caused different reactions, from claiming the need of being properly informed as to where the cameras are placed to saying that it's better not to know where they are.
Apparently, the initiatives oriented to protect citizen safety are viewed as more positive although there are doubts about their actual effectiveness.

Ranking of Different Types of Privacy

In the final section of the focus groups, participants were asked to complete a handout that was designed to rate four types of privacy both in terms of the level of importance in protecting and the degree to which these types of privacy are under threat today.
The handout is included in the appendix. The four types of privacy were:

- Bodily privacy (e.g., being watched or monitored without your knowledge or permission);
- Communication privacy (e.g., someone listening to your conversations or reading your emails without your knowledge or permission);
- Informational privacy (e.g., controlling what information is collected about you); and
- Territorial privacy (e.g., not being disturbed at home, being able to have times when you are completely alone, away from anyone else).

RANKING OF DIFFERENT TYPES OF PRIVACY

	RANKING			
	Bodily	**Communication**	**Informational privacy**	**Territorial privacy**
Focus Group 1				
Total Respondents	10	10	10	10
Level of importance				
Most important (1)	7	1	2	1
(2)	3	4	1	2
(3)	1	5	3	1
Least important (4)	0	0	4	6
Average	*1.60*	*2.40*	*2.90*	*3.20*
Level of threat				
Most under threat (1)	3	3	4	0
(2)	3	3	2	2
(3)	3	4	2	1
Least under threat (4)	1	0	2	7
Average	*2.20*	*2.10*	*2.20*	*3.50*
Focus Group 2				
Total Respondents	10	10	10	10
Level of importance				
Most important (1)	1	5	1	3
(2)	4	4	1	1
(3)	4	1	3	2
Least important (4)	1	0	5	4
Average	*2.50*	*1.60*	*3.20*	*2.70*
Level of threat				
Most under threat (1)	2	4	4	0
(2)	4	3	2	1
(3)	3	2	2	3
Least under threat (4)	1	1	2	6
Average	*2.30*	*2.00*	*2.20*	*3.50*
Focus Group 1 + 2				
Total Respondents	20	20	20	20
Level of importance				
Most important (1)	8	6	3	4
(2)	7	8	2	3
(3)	5	6	6	3
Least important (4)	1	0	9	10
Average	*2.05*	*2.00*	*3.05*	*2.95*
Level of threat				
Most under threat (1)	5	7	8	0
(2)	7	6	4	3
(3)	6	6	4	4
Least under threat (4)	2	1	4	13
Average	*2.25*	*2.05*	*2.20*	*3.50*

Conclusions

Both companies and government are more aware of the control issue; it is generally perceived that there is less and less privacy. There are different means to exercise this control as for example "security". The idea that everything is allowed in the name of security is accepted although with resignation and criticism.

Also, control is linked to new technologies. Technological progresses are perceived both:

- Positively, since they bring benefits of convenience and quickness, and
- Negatively, as another mechanism of control.

We noted two different attitudes when approaching the control and privacy issue:

- On the one hand, we observe a more demanding and complaining attitude rooted in more attitudinal personal values.
- On the other hand, we perceive a more conformist and passive attitude based on the conviction that nothing can be done or, in any case, that benefits prevail over inconveniences.

Workers and travellers are less critical towards control measurements. They experience privacy intrusion, at a professional level, as something inherent to their profession that can't be rebelled against.

Whereas consumers and citizens, in general, see it as an "attack" against their personal life, and thus have a more proactive approach (like going to consumer associations or simply refusing to give some private data).

In any case, "to be informed" is claimed in both groups, that is to say, they manifest that to be informed about any control measurement enables them to be free to choose between accepting it or not. In short, to be informed is experienced as being free and not obliged.

Appendix: Moderator's Guide

Globalization of Personal Data Project Focus Groups
Moderator's Guide

1.0 Introduction (5 minutes)

- Moderator explains the purpose of the research and who is the client [READ QUOTE]:

  "The main objectives of the focus groups are to provide the research team at Queen's University in Kingston, Canada with qualitative findings in relation to understanding how individuals view the larger study's area of research that deals with the Globalization of Personal Data. The findings from the qualitative phase will help shed light on the issues and how they are perceived, with a view to helping frame questions for the quantitative survey component of the project."

- Moderator explains that the discussion is being audiotaped and/or videotaped as the moderator cannot take good notes during the focus group.

- Moderator explains that participants may be observed by member of the research team. **[PLEASE EXCLUDE IF NO OBSERVER WILL BE PRESENT]**

- Confidentiality: Moderator explains that the findings from the focus groups are kept confidential. No full names will be associated with any information provided in this discussion group. The report will simply describe patterns of opinions over the series of focus groups..

- Moderator explains that participation is voluntary and that participants are free to withdraw at any time without penalty.

- Moderator explains that participants are not obliged to answer any questions they find objectionable or which makes them feel uncomfortable.

- Moderator explains the format and "ground rules": there are no wrong answers/no right answers, okay to disagree, individuals are asked to speak one at a time.

- Moderator explains his/her role: raise issues for discussion, watch for time and make sure that everyone gets a chance to speak.

- Moderator asks participants if they have any questions before beginning.

- Participant introductions: Moderator asks participants to introduce themselves by their first name only and to say a little bit about their background (e.g. occupation/status).

2.0 Perceptions and Experiences with Privacy Issues (35 minutes)

When you hear the word "privacy", what is the first thing that comes to mind? [Moderator instructs participants to write down the first thing that comes to mind.]

And when you hear the word "security", what is the first thing that comes to mind? [Moderator instructs participants to write down the first thing that comes to mind.]

Respondents are then asked to read what they wrote down about "privacy" and "security".

People often talk about privacy as a value. What is a value [PROMPT: freedom, equality are often cited as values]? What about privacy as a value?

In our surveys, we often ask people about privacy, and whether or not they feel that they have less privacy in their daily life than they did five years ago. How would you answer this question?
- Can you tell us why you feel that way?
- In what areas do you have less privacy?

How concerned are you about your privacy today? ·

- What kinds of things do you do to protect your privacy?
- Where do you generally get your information about privacy issues?
- Have you ever discussed these issues with family, friends?

How have your views changed in the past five years? In what ways?

- What prompted these changes? Is anything different since September 11th?

Has anything you have seen in the media (TV, radio programming, newspaper, magazines, online information or advertising) prompted these changes? How so?

Have you ever experienced a serious invasion of privacy?

- What kind of invasion of privacy was it?

Can you give me some examples of privacy invasions?

- Invasions in your day-to-day lives?
- Invasions by government?
- Invasions by companies?
- Invasions in the workplace?

What are some other ways that your privacy could be compromised?

- [Prompt if necessary: identity theft, credit information, credit card, financial information, surveillance cameras, tracking of purchases].

Are some groups in society more susceptible to invasions of privacy than others? Which groups? [PROMPT: Low-income, visible minorities, ethnic groups] Why do you say that?

3.0 Expectations Regarding Privacy Issues in the Future (15 minutes)

How likely is it that you will actually experience a serious invasion of your personal privacy over the next five years? What type of invasion could you see happening?

Compared to today, do you think that the threat of an invasion of your personal privacy will be greater or less in ten years from now? Why do you say that?

What do you think may not be as private in the future?

If I asked you to pick one thing, what would you say is the biggest threat to your privacy in the future?

How do you think technology will affect your personal privacy in the future?

4.0 Awareness of and Attitudes towards Privacy Technologies and Legislation (30 minutes)

Technologies

How much do you rely on electronic or computer-based technology in your daily life, either at home or at work?

- What types of technology do you use?

How confident would you say you have enough information to know how technology might affect your personal privacy? What about the Internet?

How could the Internet affect your privacy? And what about email?

Are you aware of things that you could do to protect your privacy while on the Internet?

- Have you ever done anything to protect your privacy while on the Internet?

Have there been any changes with respect to the use of these technologies by companies/governments in the past few years when it comes to your privacy?

- In what way have things changed?
- What do you think prompted this change?

Legislation

What things exist to protect your privacy today? What laws exist?

Are you aware that there are federal privacy laws that place strict restrictions on how federal government departments use personal information, including restrictions on the sharing of personal information?
- To what extent do you believe these laws are effective at protecting your privacy?

What about laws that place restrictions on how companies use personal information, including restrictions on the sharing of personal information?
- To what extent do you believe these laws are effective at protecting your privacy?

[As some of you mentioned] some measures aimed at increasing security are, at times at the expense of privacy. Do you think this is currently the case?
- Specifically, what security measures compromise privacy?
- On balance, do you feel these measures aimed at increasing security are justified?
- What about in the future? Do you expect the emphasis will be more on "security" or "personal privacy"?

5.0 Privacy Issues Specific to Workers (25 minutes)

To what extent do you think companies keep track of the activities of employees while they are in the workplace?
- Are they tracking how much time employees spend online, maintaining a list of websites employees visit and information entered? Emails sent or received?
- Should they be allowed to monitor these types of activities of their employees? What types of activities? Why? Why not?
- What is and isn't personal information in the workplace?

Do you know if your employer uses any methods to track the actions of their employees? How do you feel about this?

Do you believe businesses are required to inform employees and prospective employees of different methods they may use to monitor workplace activities?

Should employers be able to monitor all their employees equally or should they be able to target or exempt individuals or groups of employees from monitoring?

6.0 Privacy Issues Specific to Travelers (25 minutes)

Do people who travel a lot face any privacy-issues that non-travelers do not? What about those that travel regularly between other countries? What types of things are different?

To what extent should the Government of [insert your country] track the movements of its citizens as they exit or re-enter [insert your country]? Should information collected be shared with other governments or international agencies? Why do you say that?

After September 11th, the United States required advance information on air travelers destined for the United States. As such, the federal government of [insert your country] had to comply and ensure that this information is transmitted ahead of time.
- Were you aware of this requirement? What, if any concerns, do you have with this?
- What do you think of the fact that [insert your country] had to comply (i.e., they did not have a choice)?

7.0 Privacy Issues Specific to Consumers (25 minutes)

How many of you have ever participated in a customer loyalty program such as Airmiles?
- What is the purpose of these programs?
- Why do you participate?
- What type of personal information do they collect? What do they do with this personal information?

- Can they sell this personal information to other companies? Under what circumstances can they? [FOR THOSE IN LOYALTY PROGRAMS] Have you given consent?

As some of you may know, when individuals take part in a loyalty program such as Airmiles, each time they use their card to collect points, the Airmiles company keeps track of the items they have purchased. These companies can then sell this "purchasing behaviour" information to other companies participating in the Airmiles loyalty program.

- What do you think of a company being able to track purchases?
- What do you think of them being able to transmit that information to other companies?
- What kinds of things is it ok for companies to monitor?

Have any of you ever made a purchase over the Internet? Why/why not?

- What prompted you to make your first purchase over the Internet?
- Did you think it would be safe?

What about privacy policies on websites and e-commerce websites in particular?

- What do you think of these policies?
- Who actually reads them?
- Are they adequate measures of privacy protection? Are they all equal, or does your view about the privacy policies depend on the company? Why?

8.0 Privacy Issues Specific to Citizens (25 minutes)

Let's turn to the issue of surveillance cameras. How are surveillance cameras being used in your community? How are they being used elsewhere in the country?

- Where are they located?
- What are they used for?
- Who operates them?
- What purpose do they serve?

In London England, and in some Canadian communities, such as Kelowna B.C., police are using surveillance cameras to monitor public places in order to deter crime and assist in the prosecution of offenders. In fact, there are roughly 150,000 surveillance cameras operating in London.

- What do you think of surveillance cameras in public places? What are the pros? What are the cons?
- Do you think this is an effective way to reduce crime?
- Are their other more effective ways?

What would you think if a large city like [insert city where focus groups are being conducted / large city from your country] was to follow the lead of a London, England and introduce surveillance cameras all across the city?

- Good idea? Bad idea?
- Would you have any concerns? What?
- How comfortable are you with the idea of being monitored by a police surveillance camera as you walk down a street or go to a park?

9.0 Concluding Questions (10 minutes)

Have participants answer the handout (on following page).

Is there anything else you would like to add before we end the discussion?

THANK YOU FOR YOUR PARTICIPATION!

HANDOUT: ATTITUDES ON PRIVACY

Some privacy experts talk about four different types of privacy: bodily privacy, communication privacy, informational privacy, and territorial privacy.

How would you RANK these different types of privacy in terms of how important it is for you to ensure that your privacy is maintained in these four areas? [Please rank the four types listed below with a 1 to 4, where 1 is most important and 4 is least important].

Bodily privacy (e.g., being watched or monitored without your knowledge or permission)

Communication privacy (e.g., someone listening to your conversations or reading your emails without your knowledge or permission)

Informational privacy (e.g., controlling what information is collected about you).

Territorial privacy (e.g., not being disturbed at home, being able to have times when you are completely alone, away from anyone else)

And how would you rank the same four types in terms of the degree to which these areas of privacy are under threat for you, personally? [Please rank the four types listed below with a 1 to 4, where 1 is most under threat today 4 is least under threat today].

Bodily privacy (e.g., being watched or monitored without your knowledge or permission)

Communication privacy (e.g., someone listening to your conversations or reading your emails without your knowledge or permission)

Informational privacy (e.g., controlling what information is collected about you).

Territorial privacy (e.g., not being disturbed at home, being able to have times when you are completely alone, away from anyone else)