Ipsos-Insight
The Worldwide Qualitative Research Company

Project „Sherlock Holmes”

Globalization of Personal Data Project – International Survey

Qualitative Research
2 Focus Group Discussions

Executive Summary of the Hungarian research

Commissioned by

Ipsos NA

Carried out by

Ipsos Szonda

December 2004

TABLE OF CONTENTS

1. INTRODUCTION

Ipsos Szonda Hungary was hired by Ipsos North America to conduct two focus group discussions in support of the Social Sciences and Humanities Research Council-funded Globalization of Personal Data Project.

This research is an international study on privacy attitudes, operating both qualitative and quantitative methods. The first phase of the project was qualitative one, applying focus group discussions in advance of commencing the quantitative phase. This summary is based on results of the qualitative research. The main objectives of the focus group discussions were:

- To determine the respondents' perceptions and experiences with privacy issues.
- To understand what kind of perceptions and experiences determine the respondents' expectations regarding privacy issues in the future.
- To explore the elements of awareness of and attitudes towards privacy technologies and legislation.
- To know the respondents' attitudes and opinion concerning:
    - the keep tracking and the monitoring of the employees in the workplaces;
    - the information sharing between the governments about the travelers;
    - the information sharing between the companies about the consumers;
    - the surveillance cameras in the public places.

2. RESEARCH METHODOLOGY

2.1 Methodology

The research was carried out using the focus group discussion method, which, due to its duration and techniques, makes it possible for respondents to express their opinions and experience in detail, thus we could get an accurate and deep insight into the motivations and attitudes of group members.

Focus Group Discussion is a qualitative research method where the duly selected members of the target group take part. It is suitable to gain answers to all 'reasons why' questions in depth and meet issues concerning motivations, attitudes and aversions.

Traditional focus group is an interview technique in which the adequately selected members of the target group participate in a discussion. The advantage of the method, in contrast with quantitative research, lies in the interaction of participants, which, owing to the adequate process of selection, takes place in a realistic group situation. Another great strength is that because of the inner control of the group, they do not talk in clichés and do not choose stereotypes, but give good reasons for their decision – they also have time for that since group discussions generally last from one and a half to two hours.

The group discussions, which were carried out according to a guide that had been prepared by Queen's University were lead by a specifically trained moderator. In this research the number of respondents was 10 persons per group. Group Discussions were audio- and video-recorded.

2.2 Sample and timing:

Table 1

Details of the Focus Groups – Sample and Timing

Location	Groups	Date
Budapest	Workers – Travellers	December 10th, 2004
Budapest	Citizens - Consumers	December 14th, 2004

- Workers
  - Full time workers
  - Currently have access to the Internet at work
  - Use the Internet for work related activities "daily/almost daily" in a typical month
  - Range of company size (small, medium, large)
  - Range of positions (administrative, management)
- Travellers
  - Traveled by air at least once in the past year for business reasons
- Consumers
  - Purchased a product or service over the Internet before
  - Primarily responsible for most of their household's shopping needs
- Citizens
  - Hungarian citizens
  - Range of age groups
  - Range of incomes levels
  - Range of education levels
  - Range of household types

3. KEY FINDINGS

3.1 Perceptions and Experiences with Privacy Issues

To give an interpretation of the results obtained in the Budapest focus groups we must first consider a special feature of the Hungarian language. There is no single-word equivalent for 'privacy' in Hungarian, so during the discussions the following terms were used: 'protection of personal data' and 'disposition over and control of the use of personal data'. For a proper interpretation of the answers we also have to consider the fact that in Hungary today a great importance is attached to issues related to the protection and possible use of personal data. This importance is also reflected in the respondents' perceptions and experiences and is present not only at the level of everyday social interactions, but also in the media and in the communication between institutions and individuals.

During the initial phase of group discussions we asked the respondents to write down words, sentences, thoughts and feelings which came to their minds first regarding the terms 'privacy', and then 'security'. This task was completed individually so that the spontaneous associations are not influenced by other group members. The results are shown in the Appendix. To give a short summary, the associations can be grouped into the following categories:

- personal and civil rights in general, for the protection of which the legal institution of the 'ombudsman' is responsible in the modern constitutional state (these include protection of data related to private life, career, religion, world view, material circumstances, age, property, ancestry, and sexual identity);
- data theft and data trade (banking, Internet);
- the dichotomy between private life and the public sphere; the antagonism between what is official and what is not;
- secret; protections against abuse and defencelessness; confidentiality, private; own.

Fields mentioned most often by respondents regarding the term 'security':

- a life without fear, calmness;
- public order, personal safety, material security;

- children, family;
- terrorism;
- insurance – security;
- security of data stored in computers; password.

Respondents perceived a general tendency that compared to five years before they and their private data were subjected to an ever-increasing amount of attacks by various companies, state institutions and political parties. However, they also emphasized two other tendencies counteracting the one mentioned above. First, in the past 5-10 years - at the same time when the attacks multiplied - a number of institutions were established to protect individuals and their personal data. Second, individuals themselves pay much more attention to possible threats against and abuse of their private data. These two tendencies are further enhanced by the fact that privacy-related issues are widely discussed by the public. Respondents told they obtained information about privacy-related issues from the press, the Internet, TV, and the radio. The majority of them referred to these issues as one emerging even in conversations with family members and friends.

Group members had some difficulties with identifying privacy as a value, only when facilitated by specific questions could they relate it to freedom and equality. Some of them considered the term ‘value’ from the viewpoint of data abusers, interpreting it as the financial value these data have for them.

3.1.1 Personal Experiences and Concerns

Respondents in both groups shared many of their specific personal experiences. These can mostly be categorised into the six following fields:

- political parties trying to reach voters directly (by sms, mail and telephone calls) in times of elections and other major political events;
- a various companies contacting them by postal mail, telephone or e-mail to market their products;
- purchases by credit card;
- tapping of wired telephones, the possibility of being located if one uses one’s mobile phone;

- official institutions trading with their clients' data;
- abuses of identity card and identity number;
- attacks to obtain data stored in computers.

Regarding the first two fields respondents complained about political parties and various companies knowing their names, addresses, phone numbers, sometimes even what purchases they made recently. They viewed this as very disturbing and discomforting, making them feel a constant target and under pressure.

Regarding purchases by credit cards and mobile phone use respondents mostly made grievance of the possibility of being tracked as an individual. A member of the 'Consumers-Citizens' group told that some vendors, if the price of their product is not fully paid by credit card due to some mistake, can take the remaining amount from the consumer's bank account without the compliance, the PIN number and even the notification of the customer. This process was considered unlawful and abusive by both the respondent and the other group members. Several respondents told that they read in the news or heard from friends about instances when telephone conversations were recorded. It is important to note that in news programmes on TV currently give a wide coverage of such issues, and of the storing and temporary archiving of sms and mms messages via mobile phones.

Respondents were furious about official institutions (like the Ministry of Interior Affairs or the tax authority) selling their data to various commercial companies. They also complained about the careless data management in these institutions. Respondents in both groups mentioned specific instances that were covered in the media.

Abuses of identity cards and identity numbers, and identity theft were also mentioned frequently. One respondent related a case when her husband's identity card was stolen and used for a car hire-purchase. When the instalments were not duly paid, her husband received the vendor's demands for payment.

We also wanted to know which groups in Hungarian society respondents think are more susceptible to invasion of privacy than others. Respondents primarily mentioned groups that somehow differed from the average: in the first place people of higher social status and characters in public life. They attributed this fact to the uninhibited activity of Hungarian tabloids publishing articles and photos seriously violating privacy rights. Other groups mentioned were the most defenceless groups in today's Hungarian society: the homeless, the

poor and the undereducated - with an addition of the view that the effects of being a member to these groups can be further aggravated by belonging to an ethnic minority. The perception of a third group susceptible to invasion of privacy was related to lifestyle: respondents here mentioned people using credit cards, mobile phones and the Internet very often.

3.1.2 Protecting Personal Privacy

It is interesting that while respondents showed a considerable involvement in the topic investigated, they were positively uninformed about the possible ways their privacy could be protected. Group discussions converged to a view that a single individual can not do much about protecting his/her privacy with the exception of a very few strategies mentioned. These latter included minimizing the amount of official communication, orders, and purchases as well as giving false data to protect themselves from possible abuse. Other strategies involved establishing firewalls and installing data-protection software on their computers, also providing some sense of security.

In general, respondents seemed to express less trust and openness in their everyday behavioral patterns. At the present it seems these are the only means they use to defend against an ever-increasing number of attempts at invading their privacy.

3.2 Expectations Regarding Privacy Issues in the Future

During group discussions, respondents' expectations regarding the future were also assessed. A special emphasis was put to future trends and tendencies, development of protection strategies and possible changes in the privacy – security equilibrium.

Respondents all agreed that much more intensive attempts at invasion of privacy are to be expected in the future and that the value of databases describing various aspects of individuals' lives will steadily increase. Some even speculated that data theft and trade as well as identity theft would be the leading criminal acts in the future. Regarding this topic, respondents in both groups raised the issue of cloning as a means to general and complete identity theft, which they thought would be the most professional way of abusing private data.

Besides an increase in the number of attempts at invading privacy, respondents also considered the development of privacy protection as a future tendency, including specialised

institutions and protective systems. They expected a similar process in the field of privacy as that of the competition between car-theft and car-alarm systems.

Respondents were mostly concerned - and impressed - by the possibility of the linking of data stored in various computer networks and thus the emergence of a global database. When asked about what they considered the greatest danger to their privacy, most of them told it was the development of computer data storage systems. Other sources of danger mentioned were:

- credit cards
- mobile phones

Almost all respondents prognosticated that measures aimed at improving security would be put into effect, most of them also mentioning that this would weaken and erode privacy. However, they viewed this tendency as more desirable than the other way around – when confronted with a choice between privacy and security, all of them considered the latter as more important.

3.3 Privacy Technologies and Legislation

3.3.1 Technology

Technical development was mentioned spontaneously by respondents in both groups as the factor exerting the most influence on the management of personal data, and by many as the main source of danger.

Respondents attributed high importance to the danger of a global data network getting into the wrong hands e.g. by actions of computer hackers. Individual means of protection were judged‘impossible’ and ‘unfeasible’, with the only solutions being installing firewalls and anti-virus software as well as giving false information when asked about their personal data.

3.3.2 Legislation

The results of the study clearly show that respondents have only a very small amount of specific information and knowledge about laws protecting privacy. All of them know that

such laws exist, but with one single exception they could not list any of them. The only regulation they knew that the individual has to provide personal data only to the police - requests for personal information by any other institution can be denied. Specific examples mentioned were the process of ticket-inspection at Budapest Transport Company, and mobile phone purchases.

Respondents did not know the laws regulating how government institutions and commercial enterprises may handle personal data. However, because their experiences regarding the invasion of privacy by these they thought these laws cannot provide effective protection of their privacy. Thus, in general they were rather sceptical towards the law as a means to protection.

When asked about why they don't seek more information in this field they distanced themselves from the problem, saying that they themselves had not yet been subjected to invasion attempts that were serious enough to take legal action. They seemed to consider legal action as a last remedy to possible everyday grievances. They mainly knew those parts of the law that prescribe their duties, but are quite uninformed about those about their rights.

3.4 Privacy Issues and Workers

Respondents categorised as workers were asked mostly about surveillance systems at their workplaces. All of them told they had encountered such systems at their workplaces. The mentioned the monitoring of web-surfing and e-mails, doors accessible with chip cards and the video surveillance of certain areas. Two respondents told their postal mail was opened in the mail distribution centre even if it was addressed to them personally.

Very different patterns of opinions emerged regarding the video surveillance of employees. On the one hand, respondents found it 'frustrating', saying the continuous surveillance deprives them of a sense of having some 'defence' and erodes the borders separating the individual and his/her space from the collective. On the other hand, they said they had managed to adapt to surveillance. Almost all of them said that while the introduction of surveillance had been disturbing and had met with resistance on the part of the employees, eventually they got used to it and are not disturbed by it anymore. They also made a distinction whether it is only a larger space or a frequently used door (e.g. the main entrance) that is surveyed, or it involves all activities of every single employee.

Regarding workplace surveillance respondents considered it very important that different groups of employees be not discriminated in this respect. Thus, if correspondence by certain colleagues is surveyed and controlled, then this rule should apply to all people working there. One respondent told he/she considered the surveillance of just one or two workers as rightful if it was aimed not at the employees but rather at the place they work at, or if surveillance increases the security of the employee, e.g. in case of a bank cashier.

Respondents also thought it was important to inform new employees about the surveillance policy of the company or institution they would be work at - first because they thought it was unethical to withhold such information, and second because they thought that in order to behave appropriately and observe the rules workers should know the principles ruling life at their workplaces, these principles including the policy regarding employee surveillance. In general, most respondents judged information given to new employees at their workplaces as appropriate, but they were discontent with the lack of communication when surveillance had been introduced.

Regarding what constitutes personal activity, and what can be considered as non-personal some respondents cited the regulation according to which an employee working constantly at the computer has the right for a 10-minute break every hour. They thought that their activity during these periods or lunch breaks belongs to the personal sphere, thus employee surveillance during this time is rather problematic.

3.5 Privacy Issues and Travellers

Travellers did not feel more involved in issues regarding privacy than any other groups: they thought these issues emerge in their case just as often as with any other people.

Some of them thought that tracking individuals is quite feasible - first because mobile phones give information about where they are used (respondents thought it is given not only to the user, but also to mobile service providers), and second because by bringing pieces of information about passport controls at airports together it is easy to reconstruct one's route. However, all of them said they were not as much important as to be tracked by all of these methods.

The majority of respondents knew about the regulations introduced in the USA after September 11th, as they were covered in the news media. On the one hand, they were not disturbed by these regulations, as their attitudes mostly followed the logic of *'it only disturbs*

those that have something to hide'. On the other hand, they would expect it to be based on reciprocity rather than being unilateral. Thus, they thought Hungarian authorities should apply the same measures to foreign citizens, including Americans, travelling to Hungary.

Three respondents had consumer cards issued by air traffic companies (Malév, Swissair, and Lufthansa), and all of them knew about such loyalty bonuses – most group members mentioned the SMART-card by Shell. Although all respondents agreed that companies offering loyalty bonuses most probably give away their personal data to other companies, their attitude was primarily influenced by their perception of these loyalty bonuses as 'rewards', making their opinions positive about them. Altogether, 'Travellers' seemed to have weighed the pros and cons and made a judgment that due to the bonuses loyalty programmes were still worth joining.

3.6 Privacy Issues and Consumers

Two members of the 'Consumers' group participated in a loyalty programme. Like the 'Travellers', they also mentioned the SMART-card and a consumer programme by Nestlé. The primary reason for participation was the opportunity for bonuses. Respondents were very content regarding the management of personal data obtained by companies. They did not have any objections against their personal data being stored, processed, and occasionally given away to other companies.

Respondents were also asked about what products or services they used to order via the Internet. They mostly mentioned ordering pizza, DVDs, books, computer programs including anti-virus software, as well as products and services by their mobile phone service provider. Male respondents objected to the practice of asking for a lot of personal data by Internet vendors. If possible, they prefer to order from the vendor asking for the minimal amount of personal information. Thus, it was primarily males that distrusted Internet shopping. One of them even mentioned a protective strategy of having a separate bank account for such purchases, each time containing only the exact amount of money necessary for the next purchase.

Reasons for Internet shopping mentioned by respondents were laziness, low prices, and an opportunity for comfortable and quick solutions for people lacking time.

Privacy policy on websites and e-commerce websites were known by none of the respondents, although some of them mentioned the lengthy 'Terms and Conditions' at the end

of which they have to choose the 'I agree' option (opposed to the 'I disagree' option) to place the order. However, none of them have ever read these texts, first because they found them rather lengthy, and second because most of the time they are in English, and even if the respondents speak English the time to read the text would make this way of shopping less desirable, as it is chosen for its quickness in the first place.

3.7 Privacy Issues and Citizens

Before we turn to reviewing the results of the 'Citizens' group we must note that in certain districts of Budapest an area surveillance system was introduced about two years ago. Thus, respondents based their opinions on their real-life experiences, and not only on placing themselves in hypothetical situations.

Respondents related to these cameras and area surveillance systems very positively without exception. They have a wide knowledge about these systems. They saw the cameras in shops, shopping malls and in banks, as well as in public places like streets and squares in Districts VI, VII, and VIII. They also knew that the proprietors of these systems are the respective local authorities, while their operation is the responsibility of the police. This was entirely approved by all respondents, first because they trust the police, and second because it is the police that can take official measures in case a criminal act is detected.

Area surveillance cameras in public places were seen by respondents as improving public security in districts that had had a very bad reputation in this respect before. For example, respondents ascribed to these systems the fact in District VIII (Józsefváros) formerly prevalent criminal acts like prostitution, pickpocketing, robbery, and car theft were driven back or disappeared almost entirely. They gave the following pros of area surveillance systems:

- they deter criminals and improve public security; crime is driven back (especially car theft, prostitution, street violence, and pickpocketing);
- data obtained by these systems can be valuable for statistical purposes (e.g. attendance at museums and public institutions can be measured; traffic can be counted etc.);
- they can also be installed by private individuals, e.g. people living in the same apartment house to protect their property e.g. from burglary;

- one respondent said it could also provide help to individuals – he related about a political rally organised by the far right; authorities removed all cars parking in the square where the rally was to be held in order to avoid property damage. The area surveillance camera recorded which cars parked in no-parking areas, and in principle, only the owners of these had to pay for the transportation. (Unfortunately, the process was not so smooth in practice: our respondent eventually had to pay despite of his car being parked regularly.)

The cons of area surveillance systems mentioned were not so many, and related to issues respondents did not judged so important:

- the camera can record events which the individual recorded would have wanted to remain secret (the specific example mentioned by the group was an extramarital relationship);
- a young respondent (still a student) mentioned another counterargument: one can be recorded and later charged for such minor offences like going home with friends from a night out and meanwhile consuming alcohol in a public place; or stopping one's car only for a few minutes in a no-parking place just to manage an urgent affair quickly.

When asked about the effect of area surveillance systems on their own lives and everyday behavior in public places, respondents said they did not make a difference regarding any of their usual habits - they act as if no cameras were present. Only one of them said he would be more reserved when walking with his sweetheart in Margitsziget if there were cameras on all trees in the park.

3.8 Ranking of Different Types of Privacy

In the final section of the focus group discussions, respondents were asked to complete a handout that was designed to rate four types of privacy: bodily, communication privacy, informational privacy and territorial privacy.

The following tables clearly show the results concerning the ranking of different types of privacy in the Group 1 and Group 2, and in the whole sample.

Table 2

Ranking of Different Types of Privacy

	Ranking			
	Bodily	*Communication*	*Informational*	*Territorial*
Budapest Group 1 ("Workers" and "Travellers")				
Total respondents	10	10	10	10
Level of Importance				
Most Important (1)	2	4	1	3
(2)	2	3	2	3
(3)	3	3	2	2
Least Important (4)	3	0	5	2
Average	2,7	1,9	3,1	2,3
Level of Threat				
Most Under Threat (1)	2	2	5	1
(2)	2	7	1	0
(3)	2	1	3	4
Least Under Threat (4)	4	0	1	5
Average	2,8	1,9	2	3,3

	Ranking			
	Bodily	*Communication*	*Informational*	*Territorial*
Budapest Group 2 ("Citizens" and "Consumers")				
Total respondents	10	10	10	10
Level of Importance				
Most Important (1)	2	4	2	2
(2)	0	2	4	4
(3)	2	4	2	2
Least Important (4)	6	0	2	2
Average	3,2	2	2,4	2,4
Level of Threat				
Most Under Threat (1)	2	4	2	2
(2)	2	5	2	1
(3)	3	1	4	2
Least Under Threat (4)	3	0	2	5
Average	2,7	1,7	2,6	3

	Ranking			
	Bodily	*Communication*	*Informational*	*Territorial*
Budapest Group 1 & Group 2				
Total respondents	20	20	20	20
Level of Importance				
Most Important (1)	4	8	3	5
(2)	2	5	6	7
(3)	5	7	4	4
Least Important (4)	9	0	7	4
Average	2,95	1,95	2,75	2,35
Level of Threat				
Most Under Threat (1)	4	6	7	3
(2)	4	12	3	1
(3)	5	3	7	6
Least Under Threat (4)	7	0	3	10
Average	2,75	1,8	2,3	3,15

Legend:

Most Important / Most Under Threat
Least Important / Least Under Threat

Looking at the results in the tables above, it can be concluded that:

- Respondents rated communication privacy as the most important, and the rating averages indicate that they also perceived it as the field being most under threat.
- Members of the 'Citizens and Consumers' group rated bodily privacy, while 'Workers and Travellers' rated informational privacy as having the least importance.
- Rating averages in both groups reveal that territorial privacy is considered the field being the least under threat.

4. CONCLUSIONS AND IMPLICATIONS FOR THE QUANTITATIVE PHASE

From the two group discussions the following conclusions can be made:

- Respondents see the social discourse regarding the protection of privacy as a problem of the present day and as one which they are personally involved in.
- Their reasoning about this subject is influenced by the following factors:
    - the topic of privacy is widely discussed in the media (press, TV, radio, Internet);
    - just like in Western Europe, the use of credit cards, mobile phones and computers is quite wide-spread in Hungary, and the Internet is also used by more and more people and in more and more households – questions and problems arising in these fields affect people - and thus the respondents - directly;
    - Hungary has gone through a process of switching from one political, economical and social system to another one. This process has changed almost all aspects of life, including the individual's relationship to the state, to institutions, to social groups and to other individuals. These changes entailed the emergence of questions which were not relevant before, like privacy. At the present, a kind of transition can be observed in this respect. The situation is further affected by Hungary's accession to the European Union.
- Respondents prognosticated more forceful attempts at invading privacy and stealing personal data in the future. These attempts are expected from all kinds of sources including government institutions and official bodies, political parties, but also commercial companies. The proliferation of identity theft as a crime as well as data trade and data abuse by individuals or organised crime groups are perceived as a very real source of danger.
- Regarding privacy and security respondents prognosticated a shift towards a greater emphasis on the latter, which they fully approve. This trend certainly gives rise to other questions, e.g. the possibility of large databases established to improve security getting into the wrong hands.
- The worst threats to personal data are perceived as follows:
    - The development of information technology

  - Credit card use
  - Mobile phones
  - The linking of separate databases

- Respondents do not have much information about the legislation regarding privacy, but they know and attribute a great importance to the legal institution of the ‘ombudsman’, which is seen as a pillar and a sine qua non of the modern, democratic, constitutional state.
- When they were talking about the issue it became clear that most of the respondents had already experienced more or less serious attempts at invading their privacy. Protecting personal data and the discussion thereof is a part of their everyday lives.
- Finally, it should be noted that regarding privacy a transitional period can be studied in Hungary. A study like that can be interesting because a pattern of opinions and attitudes regarding various elements of the field can be investigated in a process of gradual change, revealing the discourse between and the dynamic change in the main patterns, as well as the forces at work behind them.

5. APPENDIX

5.1 Discussion Guide

I. INTRODUCTION (5 MINUTES)

MODERATOR EXPLAINS THE PURPOSE OF THE RESEARCH AND WHO IS THE CLIENT:

> "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.

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).

II. 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?

III. 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?

IV. 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"?

V/A. 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?

V/B. PRIVACY ISSUES SPECIFIC TO TRAVELERS (25 MINUTES)

- Do people who travel a lot face any privacy-issues that non-travellers do not? What about those that travel regularly between other countries? What types of things are different?
- To what extent should the Government of Hungary track the movements of its citizens as they exit or re-enter Hungary? 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 travellers destined for the United States. As such, the federal government of Hungary 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 Hungary had to comply (i.e., they did not have a choice)?

V/C. 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?

V/D. 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 Budapest 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?

VI. 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

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].

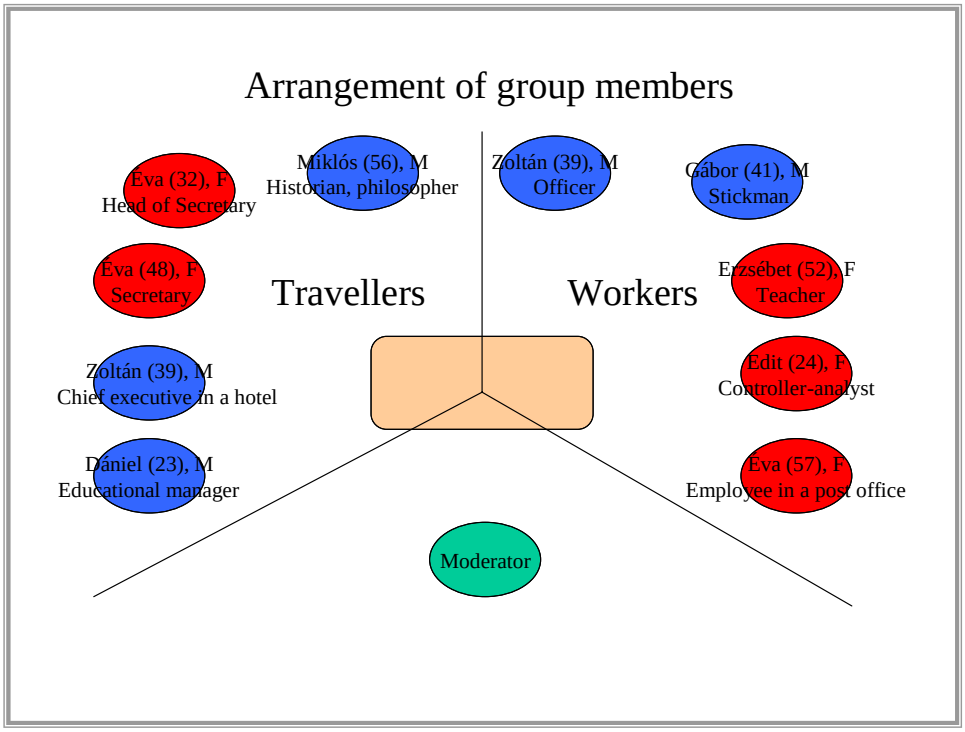
Bodily privacy (e.g., being watched or monitored without your knowledge or permission) _____

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) _____

5.2 Arrangement of Participants in Group 1 ('Workers' & 'Travellers')



5.3 Arrangement of Participants in Group 2 ('Citizens' & 'Consumers')