Globalization of Personal Data: Japan Summary Report

Prepared for

Ipsos North America

By

Table of Contents

1.0 Introduction

In order to gain greater insight into how the Japanese public regards privacy issues, Infoplan, Inc. was contracted to conduct a series of two focus groups by Ipsos North America on behalf of Queen's University (Canada) and the Globalization of Personal Data (GPD) project.

The objectives of the Japanese focus groups were to provide the GPD research team with additional insights on issues relevant to personal data, and how they are perceived from a Japanese perspective. Insights yielded are to be used when designing the subsequent quantitative portion of this project.

It should be borne in mind when reading this report that all findings contained herein are based solely on the qualitative research conducted (two focus groups in total). While efforts were made when structuring the research and while recruiting to insure that all key segments were represented, these focus groups should not be considered representative of the larger Japanese population as a whole.

2.0 Research Methodology

The research was conducted according to the following mythology and schedule:

- Two focus groups in total with 10 respondents each were conducted in central Tokyo on October 28 and 29, 2004. Each group lasted for approximately two hours.
- Respondents were recruited following qualifications defined in a screening questionnaire provided by Ipsos North America. Qualifications were adjusted slightly to match with the Japanese environment. (Qualifications listed on page 4)
- Group 1 was composed of "Workers" and "Travellers." Group 2 was made up of "Consumers" and members of the "General Public."
- A professional Infoplan moderator using a structured discussion guide provided by Ipsos North America conducted the groups.
- All participants received a cash incentive for their involvement (9,000 JPY).

2.0 Details of the Tokyo focus groups

Group	*Respondents*	*Date*	*Location*
Group 1	**Workers (5)** **Travellers (5)**	**October 28, 2004**	**Infoplan, Inc.** **Central Tokyo**
Group 2	**Citizens (5)** **Consumers (5)**	**October 29, 2004**	**Infoplan, Inc.** **Central Tokyo**

Respondents

- Each group consisted of 10 respondents from a range of ages (20-49 YO) and income levels.
- 5 males and 5 females were recruited for each group.

Group 1 qualificaitons:

Workers (5)

- Currently have access to the Internet and/or email at work
- Use the internet/ email for work related activities "daily/almost daily" in a typical month
- Range of company sizes (small, medium, large)
- Range of positions (administrative, management, etc.)

Travellers (5)

- Have made at least 2 round trips by air within the last 12 months (including both domestic and/or international flights)

Group 2 qualifications:

Consumers (5)

- All have purchased a product or service over the internet in the past or have considered doing so.
- All are primarily responsible for most of their household's shopping needs

Citizens (5)

- All have contacted a government authority at least one time within the past 12 months.

3.0 Key findings

Findings from the Japanese groups indicate that personal data/privacy issues have a low "top-of-mind" presence with respondents, although many understood that privacy and personal data issues have recently received increased media coverage. Some variations in respondents' degree of concern with the issues were witnessesed, however attitudes regarding personal data/ privacy issues tended to be mainly passive in general (most respondents had not given the issues much forethought/ concern to the topic). However, some females and the small number of respondents who had directly experienced invasions of privacy also displayed somewhat higher degrees of concern for privacy issues than average.

Perceptions and Experiences with Privacy Issues

Top of mind reactions to "Privacy" and "Security"

(Answers to respondents' self completion questionnaires is available in the appendix to this report pg 21)

Respondents' answers regarding their initial thoughts upon hearing the word "privacy" tended to focus on the following topics:

1. Invasions of privacy
2. Personal information
3. Things you do not want others to know/ secrets

Reactions to the word "security" focused primarily on the following areas:

1. Safety (free from danger)
2. Prevention/ preservation

A few respondents also made links to "internet security."

The narrow range of answer types provided may indicate respondents' high degree of understanding that personal data/ privacy issues are currently a widely discussed topic in the media. They also stood in contrast to respondents' admitted lack of deep thought given to the topics.

Privacy as a Value

Judging from post-interview questionnaire results and group discussions of the definitions of "security" and "privacy" a few respondents seemed to consider privacy and security as "rights." However, when directly questioned on weather "privacy" constituted a value, most respondents had difficulty understanding the question/ concept and instead spoke about the (monetary) value of "privacy" and "private information." This can be taken to indicate that respondents did not regard privacy as a value.

Concerning the "the value of privacy," the consensus was generally that private information would be of monetary value to marketers or swindlers/ con artists. In the ensuing discussion the problems of corporate leaks of customers' information, telemarketing and targeted swindles/ invasions of privacy were regarded as invasive and highly negative.

"If you think about it in terms of money, then I guess it has a value." G1

"Private information would have a value to con artists who run those 'it's me, it's me! Scams'" G1*

"The problem of companies repeatedly leaking information is very troublesome." G2

"I don't want to have my privacy invaded, so privacy certainly has a value to me, but it is difficult for me to describe exactly what it is….." G2

Current concerns about privacy issues

Throughout the groups respondents displayed the attitude that personal data and privacy are not frequent topics of conversation or top of mind concerns. The most commonly cited sources for information regarding privacy issue were newspapers, magazines and TV news programs. Many respondents appeared to feel that privacy was not a newsworthy subject or a point of concern for the general public unless a major information leak or other large scale invasion of privacy occurred. Nonetheless, there was a strong consensus in Group 2 (Consumers and Citizens) that privacy has been increasingly under threat. Most respondents in this group felt that their privacy has been eroded over that past five years.

**"It's me, it's me!" scams are a recent phenomenon in Japan where a con artist calls victims (Frequently elderly people) pretending to be a relative in trouble. The con artist requests the victim transfer money to a bank account with out providing a name.*

Some group 1 respondents (Workers, Travellers) felt that there had been a major erosion of privacy 1-2 years ago but that it has not changed much recently, while a few indicated they did not feel there has been significant changes in the past 5 years. Many respondents in both groups indicated they felt a slow loss of privacy was inevitable, and seemed resigned to a future with less privacy.

Sources of threats to privacy offered by respondents were most frequently technology based, especially cell phones, email and the Internet. Common technology based threats/ potential threats to privacy mentioned by respondents included:

Spam emails to business, private and cell phone email addresses

An increase in direct mails after registering for services on the Internet.

An increase in telemarketing calls to cell phones as well as fixed lines

Leakage of information from ward offices' resident registration electronic data bases *(Jukine*t)*

Leakage of information from major service providers electronic data bases (**Ex.** *Yahoo BB*: an ISP)*

Leakage of student information from school registration lists leading to marketing calls/ door to door sales from text book publishers/ crams schools

Increased numbers and variety of swindles/ scams utilizing cell phones

"These days I get a lot of bothersome phone calls on my cell phone. 5 years ago I didn't receive any of these." G2

"I thought it was safe to enter my name and address when buying online, however after doing so, there was a big increase in the amount of strange direct mail and email I received." G2.

"Some information leaked from my child's school, and we received a lot of calls from cram schools and pushy door to door text book salesmen." G2

**In Japan all citizens are required to register their domicile with their local ward or town office. Jukinet is an electronic database to facilitate the transfer of this registration information between various towns/ ward offices and prefectural governments. It was controversial when introduced in 2002/ 2003, with a few town/ward offices refusing to participate because of a fear of leaks. A few limited leaks of citizen's information have since occurred.*

** A major leak of customer information by Yahoo! BB (Japans largest broad-band internet service provider) occurred in the Spring of 2004 receiving a large amount of media coverage.*

Only a few sources of privacy loss not related to technology were mentioned by respondents including getting married and having children.

While regarding the terrorist attacks of September 11, 2001 as tragic, respondents did not see them as directly affecting their privacy in any meaningful way, and tended to regard them as a mainly foreign event. A few respondents noted however, that they understood the need for an increased level of security in public places following the events or that the felt more secure when traveling because of the extra precautions that have been enacted.

"It doesn't bother me that security it tighter now. Actually I feel more at ease because of it." G1

Prevention measures

Even though feelings of urgency regarding privacy issues were not typically displayed by most, a number or respondents in each group noted they took some preventive measures to protect their privacy. Preventative measure mentioned included:

Checking caller ID displays and only answering calls from those who are known on home phones or cell phones. (2-3 respondents in each group)

Removing ID numbers/ information from direct mail before disposal. (2-3 respondents in each group)

Shredding mail before disposal. (2-3 in each group)

Not listing phone numbers/ address information in the telephone directory (1-2 in each group)

Not entering address/ phone information when requested (online/ sweepstakes entries etc)

Not purchasing items online. (1-2 in each group)

Installing/ updating PC Internet security software. (1 in G1)

"I don't list my phone number in the phone book, because I don't want to be contacted." G2

"I don't fill out post cards and forms that ask for my address." G1

"I installed some software from Norton on my PC, but that is about all I've done to protect myself." G1

"I don't pick up phone calls from unknown sources. I have a number display function on my phone, and if I receive a call from an unknown number, I don't pick it up." G1

Information sources, personal concerns and experiences

As indicated earlier, respondents' main sources of information about privacy related issues were mass media (newspapers, magazines and TV news programs.) As such, most respondents were familiar with the recent news stories, especially controversial data leaks from government/ large corporations and sensational crimes/ scams that are frequently reported on. Many of these issues rely on the Internet (as a leaking point for information) and cell phones (as a delivery vehicle for swindles/scams by con artists) perhaps providing a base for many respondents' position that technology is a chief cause of the erosion of privacy. Examples of (technology based) invasions of privacy mentioned include:

Customer information leaks from Yahoo! BB (an ISP) and other customer service providers.

The controversial *"Jukinet"* residents' registry and recent leaks from it.

"It's me! It's me!" scams

"One ring" cell phone call back scams*

Although respondents in general were aware of these leaks and scams with a few indicating they had directly victimized, most seemed to regard them as distant events that were somewhat difficult to relate to. One respondent even noted that he had heard about information leaks so often without ever being affected, that he has become numb to them.

As noted, in each group a small number of respondents indicated they had been directly affected these leaks and scams. Interestingly, some respondents who had been victimized by data leaks only seemed to regarded them as mainly as a nuisance. Those who had been targets of scams, however, tended to react more harshly. This seems to reflect the pervading attitude of "it doesn't really concern me until something serious happens," displayed by many respondents in the groups.

"My information was leaked by Yahoo! BB. They sent me 500 yen. But nothing's has really happened since then." G2

"I received a telephone scam call on my cell phone recently. They actually claimed to be the police! It really upset me." G2

**"One ring" cell phone call back scams work in the following way. The con artist calls a potential victim on their cell phone and lets it ring only one time, sometimes at repeating intervals. Some recipients call the number back after examining their received call registry because they think they have received a legitimate phone call. The number they call however is typically registered as a telephone sex service with very high per minute rates (ex. $100/min). If the victim refuses to pay they may receive threatening phone calls or bills sent to their address that indicated they have called telephone sex services.*

Other types of invasions of privacy respondents mentioned experiencing included:

Fake telephone/ utility bill scams*

Surveillance cameras on the street

Telemarketing calls.

Compulsory company health checks.

For the majority of respondents, these were considered to be only nuisance level invasions of privacy.

"I received a false phone bill. It said I had called person I don't know in somewhere in Africa, so I just threw it away." G2

No respondents reported being victims of identity theft or stolen credit card information, and for most respondents these did not appear to be topics of concern. Nonetheless about half of all respondents in each group indicated they do not fell comfortable entering credit card information online and do not use them or use them only with a limited number of online retailers.

When probed on weather certain groups in society are more susceptible to invasions of privacy than others, responses were mixed. Many respondents suggested celebrities and politicians would be more susceptible because they faced greater scrutiny by the media. Some respondent also indicated people in lower social strata because they were considered to be less educated and more easily tricked into providing personal information or victimized by con artists.

"Politicians and celebrities are more closely observed." G1

"Less educated people will provide personal information more easily." G2

Other groups named by respondents as more susceptible to invasions of privacy included people who frequently use the internet and women who were regarded as more frequent shoppers and therefore more likely to interface with marketers.

** Fake telephone bill/ utility bill scams work in the following way. Counterfeit telephone/ utility bills that look very similar to originals are sent to potential victims requesting payment by bank transfer. Sometime even follow up telephone calls are made to those who do not pay requesting payment.*

Expectations Regarding Privacy Issues in the Future

For the future, most respondents anticipated continued erosion in privacy, especially caused by advancements in technology.

"Losses of privacy are going to gradually continue. There is nothing we can really do about it." G1

"Eventually the information is going to leak. It is hard for the people managing it to keep up with all the changes." G2

A few respondents in both groups, however, indicated they believed their level of privacy would remain about the same in the future. These respondents held that although technology would continue to advance and potentially become more invasive, that technologies to protect privacy would also advance in parallel to defend it.

"Technologies to defend our privacy will also be invented. I think our current level of privacy will be maintained in the future." G1

Types of future erosions of privacy anticipated by respondent included:

- Stolen cell phone data
- Increased number of online scams
- DNA data bases
- ID microchip implants in humans
- IC chips in personal ID cards
- Surveillance cameras on streets and in public places.
- Continued electronic Information database leaks
- Stolen internet ID's/ Login names

"I think 'Dummy cell phones' where people steal cell phone data and have charges sent to the legitimate owners will be more of a problem in the future." G1

"I think things like DNA databases or chips implanted in peoples' bodies from the time they are born will become a problem." G2

Privacy Technologies and Legislation

Technology

Most respondents admitted they were highly reliant on technologies in their daily lives, with email the Internet and cell phone being the prime examples offered. Many respondents were quick to admit that they did not necessarily know enough about the various types of technologies they use to fully protect themselves against invasions of privacy. However respondents also

seemed to feel that technologies make life easier, and unwilling to forego the benefits for the sake of improved privacy/ security. In general, respondents did not see technology itself as the root of privacy loss, but rather people who used the technologies to invade others' privacy. Nonetheless some respondents still mentioned they were unwilling to enter private information or make purchases online because they did not want their information stolen or seen. A small number of respondents however noted that while they used to be cautious about shopping online, they feel more comfortable now because they have made many purchases without ever being victimized.

"I'm not confident that I know enough. Things change so rapidly. It is difficult to keep up." G1
"I don't know enough, but I'm less concerned with it. At first I didn't want to shop online because I didn't want to enter my credit card information. But now I shop online often…It is easy and I'm comfortable with it." G2

Legislation and the Trade-Off between Privacy and Security

Awareness of privacy rights and legislation intended to protect individuals' privacy was very low in both groups. Most respondents could not name or describe much legislation intended to protect privacy and personal data other than the national constitution. About half of respondent in both groups, however, mentioned they had herd of the recent Privacy Mark Law (
) regulating how companies use personal information, when mentioned in the groups. Some respondents speculated that knowledge of relevant legislation was so low because television stations, which were expected to be a prime source of this type of information, did not air information about laws because of anticipated low audience interest. Nonetheless, respondents tended to trust that legislation to protect their privacy had already existed.

"Most of the general public is not very interested in this type of legislation, so it is not shown frequently on TV." G2
Oh yeah, I think there was a new law regulating companies' buying and selling of personal information." G1
"I don't know much about the content of privacy laws." G2

Respondents mentioned that they preferred having laws enacted to protect their personal information to having no laws at all, and expected that the presence of law would help protect them from abuses at least marginally. However respondents many noted that they did not expect the laws to fully protect them. Similarly many did not consider the government or companies to be primary violators of their citizens' privacy, but rather nefarious individuals who were unlikely to adhere to the laws. Some noted that they would have to remain personally responsible for

maintaining their privacy. It should be noted that respondents did not seem to fear the government or regard it as a violator of privacy. Rather they seemed to feel that it government would merely be incapable of protecting their privacy sufficiently.

"New laws will be more of a deterrent, but will not protect us completely. Invasions of privacy will continue, but it makes me feel better to know the government is doing something about it." G2
"Invasions will still continue. The problem is not the government or companies, but malicious individuals." G2
Government laws will not be an effective deterrent. My company's policy on handling customer information is stricter than the new laws. Some employees will still abuse the system anyway. G1

In general, respondents understood that a trade off between privacy and security exists, and many indicated they were willing to sacrifice a degree of privacy for greater security. However respondents also noted that they would not be willing give up privacy unless faced by a real threat.

"It seems like a cat and mouse game. If there is a real threat, I don't mind passing out my personal information. But I have to get something in return." G2
"I need a clear reason before I'm willing to give up my privacy. I need a real threat. When I'm outside Japan, I feel more under threat, so I don't mind giving up some privacy." G1

Privacy Issues and Workers

Most respondents appeared to widely accept employer monitoring of employees in the workplace. All but a few respondents, who worked at small companies, believed they were currently being monitored for productivity, Internet use and/ or phone calls, with the majority fully accepting it as the norm. Most respondents regarded employers as having the right to monitor employees during business hours as well as monitor employees' use of office equipment, as it was "Company's time" and "Company's equipment." The only examples of private space or property offered by respondents were personal lockers or salary information. However respondents also strongly felt that employers have a duty to inform employees that they are being monitored.
"I work in the general affairs section at my company. We are responsible for monitoring employees' use of email and phones. I know that it is done, because I do it myself." G1
"It is the company's equipment, so of course they can monitor it." G1
"Yes, employers must inform employees; otherwise it seems dishonest." G1

Although willing to accept monitoring of productivity, and office equipment use, a number of respondents mentioned they did not like idea of companies monitoring employees' physical movements, particularly when not physically inside their office, for example when taking a break or on the weekends. However, For some employees, such as bank employees who directly handle cash or teachers of young children respondents regarded the monitoring of employees as necessary, both to protect the company and employees from false accusation.

"Those who directly handle cash should always be monitored." G1

Privacy Issues and Travellers

Most respondents agreed that those who travel frequently face more privacy issues than those who do not. Chief among these issues is the fact that passport information is recorded by airlines and that passengers' luggage is scanned or physically searched. However, most respondents did not consider these to be serious violations of privacy, and many noted they felt more secure when traveling because these measures are taken.

"*I always worry before I get on airplanes. I don't feel comfortable, but I feel safer because passengers' bags are x-rayed. I want all bags to be examined thoroughly. G1"*

"Passenger information is taken by the airlines, but I think this is necessary. What if something were to happen to the plane? The airline needs to be able to contact people. I think it is best that this information is recorded." G1

Respondent tended to be pragmatic and regarded providing information to the Japanese government as a necessary step to insure communication in case of an emergency. Similarly most did not mind the Japanese government sharing this information in case or emergency or in order to prevent crimes and terrorism.

"I don't mind the government sharing this information with other governments if it is part of an anti-terrorism policy. I'm not a criminal. It doesn't affect me." G1

"It is OK to share this information with other countries. Another Japanese citizen was kidnapped in Iraq recently. Providing travellers' information is necessary for identifying people like him." G1

Most respondent were not aware that the United States government required advance information on travellers, and many wondered what type of information was being provided. Nonetheless, most assumed that only superficial information such as that that would be on the

first page of a passport would be sent, and therefore did not consider it an important issue. In general, it appeared that respondents did not think Japanese passport holders would be examined with any more scrutiny than citizens of other countries and therefore did not seem too concerned.

Some respondents also mentioned that they realized that security has become tighter at foreign airports since the September 11th terrorist attacks. However, rather than viewing this as s violation of privacy, many noted they felt safer in general because of the increased levels of security.

"Actually since the security level has incased, I feel safer when traveling." G1

Privacy Issues and Consumers

Half of respondents in group 2 were airline customer loyalty program uses with most others being members of other types of customer loyalty programs. Most respondents displayed a good understanding of the purpose of loyalty programs recognizing them as a method for marketers to collect customer data such as name, age, gender and address and to encourage repeat buying of their products. When probed on why they participate in these programs, most commented that it was in order to receive the benefits provided to participants. Most did not consider it unusual or dangerous to provide their data, especially since tangible benefits were offered.

"The programs are to encourage passengers to ride again, and to get data to make sales activities more effective." G2

"The programs are intended to collect customer data for marketers." G2

"I joined the programs so that I can get benefits such as online check-in." G2

"I joined so that I can exchange milage points for additional airline tickets." G2

"It is information like Name, age and gender. This type of information is even taken by supermarket discount clubs, so I don't mind." G2

Respondents were not aware that the data collected by through voluntarily joining customer loyalty programs could be sold, with many reacting very strongly when this was mentioned.

"Do you mean they can provide this information to direct mailing companies!?" G2

"Really? I thought only criminals would sell this type of information." G2

Similarly, most respondents did not realize that their purchases/ and purchase behavior could be tracked via memberships in customer loyalty programs or that the information could be shared with other companies. Some respondents also reacted strongly to this, while a few did not find it

unusual or surprising.

"Does this apply to supermarket cards too? Now that I know this, I won't join one of these programs again." G2

"Our current laws are not good enough. There should be laws against this type of activity." G2

"This seems normal to me. This is the type of information that feeds marketing. It's not really any different than this type of focus group." G2

Respondents who have purchased items over the Internet were also probed on their experiences. Despite initial fears about personal or credit card information leaking, many have since become more comfortable with shopping online. Many reported purchasing online for the convenience and savings in price. Respondents noted, however that they still realize that online threats to privacy exist, with some noting that they only purchase from certain sights that they regard as more secure in order to protect themselves.

Internet shopping privacy policies were regarded to be irrelevant. Most respondents admitted they either do not read them or just skim over them. Also, many respondents believed that criminals would be able to disable companies' security precautions if they were intent on it.

"I purchase online, but I don't enter my personal information online unless it is absolutely necessary." G2

"When I purchase online I have to give my name, address and credit card number. This can be dangerous. So I try to be as careful as possible." G2

"When I first started shopping online, I was really nervous about my credit card number leaking." G2

Privacy Issues and Citizens

Respondents were able to easily mention areas where surveillance cameras are used offering examples such as ATM's, train stations, busy shopping districts, and traffic cameras on streets. For most respondents, the use of these cameras, which they regarded to be primarily for crime reduction and maintenance of public safety, was regarded as acceptable.

Many respondents were aware that similar to the London example, security cameras are already used in busy urban terminals in Tokyo such as Shibuya and Shinjuku, to monitor pedestrian movement and prevent crime. Correspondingly, most respondents not seem to regard the use of cameras in these ways as unusual or a major violation of privacy. Indeed many regarded surveillance cameras as an effective deterrent against crime and supported their use.

"Having surveillance cameras installed doesn't bother me. It is important to prevent crime." G2

"The surveillance cameras are good. I know the Shibuya police recently caught a major pick-pocket by using them." G2

However, some respondents noted that the current use of these types of surveillance cameras is restricted to certain major terminal areas only. Respondents were much less comfortable with the idea of having a large number of cameras, such as 150,000, scattered throughout the Tokyo. Many mentioned that with this large of a number all of their movements could be tracked, which they considered too invasive.

"With this large of a number of cameras, they can probably track all of an individual's movements." G2
"I don't think 150,000 are necessary to prevent crime. It seems like too many." G2
"I really don't like the idea of having that many. I feel like I would be watched all the time.

Conclusions:

The main conclusions that can be drawn from the Japanese focus groups are as follows:

Respondents tend to view personal privacy as having eroded in recent years, with most feeling that it will gradually continue to do so in years to come. These erosions are largely seen as being driven by technology.

Many respondents appear resigned to a future with less privacy.

Nonetheless individual concern over privacy issues appears to be quiet low

Respondents appear to access their providing of personal data according to a type of cost/ benefit calculation. Many respondents are willing to provide information if a benefit is provided, although they are aware that threats exist.

Although familiarity with legislation is low, the government thought of as providing at least a minimal level of protection. Nonetheless most respondents do not view currently legislation as sufficient or believe the government will be capable enough to protect citizens' rights perfectly.

Despite a general attitude that citizens must take action to insure their own privacy, most citizens acknowledge that they do not know or do enough to protect themselves completely.

Appendix

Respondent profiles

G1 : Travellers and Workers

	Name	F2:Age	F3:Gender	F7:FT/PT	F7-1:Occupation	F8: Income	F9:Education	Marriage S	F11a:Child	11b:Household Ty	Respondent Type
1	Mizuno	25	M	FT	Realtor	2	4	S	N	1	Traveller
2	Osumi	43	M	FT	Housing product design	4	4	M	Y	3	Traveller
3	Akazawa	31	M	FT	Constructor/ Chief	3	4	M	N	2	Traveller
4	Asahi	23	F	FT	Real estate consultant	6	4	S	N	4	Traveller
5	Hidaka	33	M	FT	Telecommunication	5	4	M	N	2	Traveller
6	Kusakari	40	F	FT	Paper wholesaler	5	4	M	N	2	Worker
7	Urawa	35	F	FT	Temporary staff agency	2	4	S	N	4	Worker
8	Imamura	42	F	FT	Chiropractic practitioner	5	professional school	M	Y	3	Worker
9	Marume	25	M	FT	University Office	2	4	S	N	1	Worker
10	Saitou	25	F	FT	IT system	6	4	S	N	4	Worker

G2: Citizens and Consumers

	Name	F2:Age	F3:Gender	F7:FT/PT	F7-1:Occupation	F8:Income	F9:Education	Marriage S	F11a:Child	11b:Household Ty	Respondent Type
1	Simohigash	35	M	FT	IT	5	4	M	N	2	Citizen
2	Nishida	26	M	FT	Automobile related	2	4	M	N	4	Citizen
3	Nakai	26	M	FT	IT	2	4	S	N	1	Citizen
4	Tokuda	35	F	PT	Patent related business	5	4	M	N	2	Citizen
5	Ishihara	39	M	FT	Cosmetic industry	4	4	S	N	1	Citizen
6	Sasaki	49	F	HW	-	4	2	M	Y	3	Consumer
7	Kitasaka	36	F	FT	Temporary staff agency	5	4	M	N	2	Consumer
8	Kumai	42	F	PT	Transport industry	5	3	M	Y	3	Consumer
9	Terada	26	M	FT	Telecommunication	2	4	S	N	1	Consumer
10	Kanda	44	F	HW	-	6	4	M	Y	3	Consumer

Appendix: Self Completion Questionnaire Results

G1 : Travellers and Workers

Group	Resp. Number	Age	Gender	Type	1. When you hear the word "privacy" what comes to mind?	2. When you hear the word "Security" what comes to mind?
G1	1	25	M	Traveller	An individual's important information/ An individual's personal matters/ Territory (space) that others should not enter .	A system to protect personal information/ A system to prevent (protect from) crimes
	2	43	M	Traveller	Secrets/ information	Safety, a Password
	3	31	M	Traveller	Something that is violated	Something that is necessary to lead a safe (free from danger) life.
	4	23	F	Traveller	Personal information/ My room.	Safety (opposite of "danger")
	5	33	M	Traveller	Things/ matters that you don't want seen by other people.	To protect the rights of individuals and groups.
	6	40	F	Worker	Rights that each person should protect.	Processes, Methods to protect privacy.
	7	35	F	Worker	Personal information. Secrets, Things I don't want to be known by others	Safety (opposite of "danger"), Feeling of security ("free from worry")
	8	42	F	Worker	Something that should be protected	Things that convey a sense of safety (from danger) and relief (Free from worry)
	9	25	M	Worker	Something to protect	Something which secures "safety" (Opposite from "danger")
	10	25	F	Worker	One's personal affairs/ Everything related to an individual/ Things you do not want known by other people.	Things to protect myself and others.

G2: Citizens and Consumers

G2	1	35	M	Citizen	Personal information, something that should be protected.	Safeguard. Preservation
	2	26	M	Citizen	Personal, corporate	Preventing Crime
	3	26	M	Citizen	Human rights	Something that safeguards or provides a lookout.
	4	35	F	Citizen	Something to protect. Something that must be protected.	Something that is important, necessary. To protect myself.
	5	39	M	Citizen	The "Privacy mark," (A certification for handling private information) Security, Personal information	Methods/ Policies to preserve, protect personal information.
	6	49	F	Consumer	In this age it is not something that is really protected, so I feel like I have to do something about it.	I think something has to be done about this soon, but…..
	7	36	F	Consumer	Personal information/ One's personal life and way to thinking/ Something that should be protected/ □Something that can be damaged by rumors or events.	To protect, to be safe (from danger)
	8	42	F	Consumer	Something that is very personal, Thing that you do not want others to know.	Safety, and that which protects it.
	9	26	M	Consumer	Something that it talked about recently. Personal information	The internet. Home Security
	10	44	F	Consumer	Not entering an individuals personal territory.	Safety (Opposite of Danger)

Appendix: Self Completion Questionnaire Results

G1 : Travellers and Workers

Group	Resp. Number	Age	Gender	Type	Ranking of importance for different types of privacy (1=most important/ 4= Least Important)				Ranking for different types of privacy under threat (1=Most under threat/ 4= least under threat)			
					P Bodily	Q Communication	R Information	S Territorial	P Bodily	Q Communication	R Information	S Territorial
G1	1	25	M	Traveller	3	1	4	2	3	1	2	4
	2	43	M	Traveller	3	1	4	2	2	4	1	3
	3	31	M	Traveller	3	2	1	4	2	1	3	4
	4	23	F	Traveller	4	3	2	1	4	2	1	3
	5	33	M	Traveller	4	3	2	1	3	2	1	4
	6	40	F	Worker	3	4	2	1	4	2	1	3
	7	35	F	Worker	2	3	4	1	3	1	2	4
	8	42	F	Worker	3	1	4	2	4	3	1	2
	9	25	M	Worker	4	3	2	1	4	3	2	1
	10	25	F	Worker	3	2	4	1	3	2	1	4
				Total	32	23	29	16	32	21	15	32
				Average	3.2	2.3	2.9	1.6	3.2	2.1	1.5	3.2

G2: Citizens and Consumers

G2	1	35	M	Citizen	1	3	4	2	2	3	1	4
	2	26	M	Citizen	4	2	1	3	2	1	3	4
	3	26	M	Citizen	3	4	2	1	2	1	3	4
	4	35	F	Citizen	2	3	1	4	3	2	1	4
	5	39	M	Citizen	2	4	3	1	3	1	2	4
	6	49	F	Consumer	1	4	3	2	3	2	1	4
	7	36	F	Consumer	2	3	4	1	3	2	1	4
	8	42	F	Consumer	3	2	4	1	3	2	1	4
	9	26	M	Consumer	2	3	4	1	3	2	1	4
	10	44	F	Consumer	1	2	4	3	2	3	1	4
				Total	21	30	30	19	26	19	15	40
				Average	2.1	3	3	1.9	2.6	1.9	1.5	4