GLOBALISATION OF PERSONAL DATA PROJECT

International Survey

Findings from the pre-survey focus groups

- Summary Report for France -

Not to be cited or quoted without permission of the Surveillance Project

Submitted to:

Professor Elia Zureik - Department of Sociology - Queen's University

Job # 20398 FF 01 January 2005

Table of contents

1. Introduction

Ipsos Insight (France) was hired by Ipsos North America on behalf of Queen's University to conduct 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.

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 worker). Where time permitted, some of the specific questions were asked to other groups where relevant (e.g., all travellers are also citizens).

It should be kept 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 draw from them) may not be said to be representative of the larger population as a whole

2. Research Methodology

The research findings are based on the following:

- Two focus groups were conducted on December 20th and 21st 2004 and were held in Paris.

- The groups lasted approximately two hours and were held in dedicated facilities to allow viewing by clients and audiotaping.

- A total of 12 individuals were recruited for each of the focus groups: 8 were present at group 1 and 9 at group 2.

- The focus groups were divided into four categories: workers, travellers, consumers and citizens.

- The categories in each group and way in which the respondents' profiles were defined is summarized in Table 1.

Table 1
Details of focus groups

	Profiles		Date
Group 1	50% Workers	50% Travellers	December 20th 2004
Group 2	50% Citizens	50% Consumers	December 21st 2004

- **For all targets:**
  - Good spread of ages between 20-50,
  - 50% males / 50% females,
  - Range of education levels,
  - Range of household types (with children under age- of age/without children),
  - Range of income levels and positions,
  - Range of company sizes (small, medium, large).

- **Workers:**
  - Work full-time / 35 hours per week,
  - Currently have access to the Internet at work,
  - Use the Internet for work related activities "daily/almost daily" in a typical month.

- **Travellers:**
  - Travelled by air at least twice in the past year in France, to other parts of Europe and overseas.

- **Consumers:**
  - All participants must have purchased a product or service over the Internet before,
  - All participants are primarily responsible for most of their household's shopping needs.

- **Citizens:**
  - Citizens of France,
  - All have used the internet to contact a national government service in the past year.

3. Key Findings

These key findings sum-up different themes that were consistent across the groups as well as specific issues regarding the different profiles interviewed.

Generally speaking, the findings show that French people can be described as "privacy conscious", even though respondents differ in the ways and degrees of their involvement.

I. Perceptions and experiences with privacy issues

- ***"Privacy":***

- At the beginning of the groups, respondents were asked to write down the first idea(s) that spontaneously came to mind when they heard the word "privacy" (cf. Table 2 page 8).

- In French, the most accurate and juridical translation of "privacy" would be the following: "*protection de la vie privée et des données nominatives"* (protection of private life and personal data). It is important to note that this terminology is not often used in ordinary spoken language, people would rather speak of *"vie privée"* (private life). The complexity of the French definition can perhaps explain the variety of ideas that appeared during the groups.

- Indeed, in relation to "privacy", the following ideas were recurrent:

  - "Security": the guarantee of keeping one's personal data safe.
  - "Confidentiality": it is forbidden to divulge personal data.
  - "Identity": the source of one's personal data.
  - "Computing" (computing files) and "Internet": viewed as the places where personal data are collected, and, as a matter of fact, as potential threats of privacy aggressions.

- To a lesser extent, respondents also wrote down the following ideas: "intimacy" (related to private life), "freedom" (being free to monitor one's life), the media (an instance that can divulge private data) and "legislation" (about recording data on data bases).

- ***"Security":***

- Then, respondents were asked to write down the first idea(s) that spontaneously came to mind when they heard the word "security" (cf. Table 2).

- In relation to "security", the following ideas frequently appeared:

  - The word "protection" was the most common top of mind idea, in the sense of being safe: protection of people and their assets as well as protection of one's private life (especially over the Internet or while using computers).
  - Then, the word "police" was often quoted, being viewed as the institution that protects citizens against physical but also moral aggressions.

- To a lesser extent, respondents also wrote down the following ideas:
  - As for the word "privacy", the ideas of "Computing" and "Internet" also came out: recording data about people in data bases, the login and passwords used to protect oneself. As well as the notion of "International" was quoted since, because of the Internet, the threat is now also worldwide.
  - "Legislation": a legislative framework is needed to keep one's personal data protected and safe.

- ***"Privacy as a value":***

- Then, respondents were asked to define what is a "value". Most of them spontaneously thought of "moral" values such as honesty and politeness and defined a "value" as a set of rules which need to be applied and respected when one lives among others. A minority interpreted the word "value" in the sense of a "monetary" value.

- When probed about "privacy as a value", respondents stated that the word "value" was not appropriate to define privacy. They preferred to consider "privacy" as a "right", protected and regulated through a legislative framework. Others also defined "privacy" as a private and personal "property" which cannot be used by a third party without one's agreement.

Table 2

Spontaneous associations with the words "privacy" and "security"

Group	First Name	Age	Gender	Profile	1. When you hear the word "privacy" what comes to mind?	2. When you hear the word "Security" what comes to mind?
G1	Jérôme	25	Male	Traveller	Security, Property, Identity	Filing
	Jean-Louis	60	Male	Traveller	Computing files	Police
	Marie-Agnès	47	Female	Traveller	Confidentiality	Protection of people and their assets
	Melody	23	Female	Traveller	Intimacy, Media	Police
	François	40	Male	Worker	Respecting identity	Protection, Comfort
	Virginie	28	Female	Worker	Confidentiality	Protection, Police
	Daniel	55	Male	Worker	Personal information divulged for certain transactions	Confidentiality, Reliability, 1978's law on "computing & freedom"
	Lola	53	Female	Worker	Intimacy	Protection

Group	First Name	Age	Gender	Profile	1. When you hear the word "privacy" what comes to mind?	2. When you hear the word "Security" what comes to mind?
G2	Olivier	30	Male	Citizen	Individual freedom	Protection
	Christophe	28	Male	Citizen	Law on "computing & freedom"	Login, Password
	Guy	58	Male	Citizen	Internet, Administrative file	Aggression, Police, Internet
	Leila	36	Female	Citizen	Security, Audiovisual surveillance	Protection
	Aline	20	Female	Citizen	Forbidden to divulge personal data	Laws, Regulation
	David	33	Male	Consumer	Primordial, Security	Danger, Controlling databases
	Linda	49	Female	Consumer	Secret	Security
	Annick	55	Female	Consumer	Imperative security	International
	Bernard	47	Male	Consumer	Freedom, Computing	Protection

- ***Privacy over the past 5 years:***

- Respondents all shared the idea that there is less privacy nowadays than 5 years ago and felt that anyone's personal data and behaviours can be tracked and monitored:
  - Personal data can easily be used: divulged and exchanged between companies.
  - People are targeted with commercial offers (via telemarketing, over the Internet) which accurately fit their identity and their social profile.

  "We are becoming more and more 'transparent' "
  "Now it's more and more business is business"

  Some added that if tracking consumers' habits and behaviours is not a new trend (c.f. mail order selling), however, computer-based technology has enabled to record, store and exchange personal data more easily than before.

- When probed on the impact of the terrorist attacks of September 11th on privacy, respondents stated they could not directly associate the current erosion of privacy with the security measures taken after these attacks:

  - Respondents tended to relate the increase of security measures in France to sometime in the 90's, a period of time marked with specific sociological and demographic issues: recurrent problems of violence appeared in the suburbs of some big cities such as Paris and Lyon.

  - Some also mentioned security measures taken by a former conservative Minister, Mr Nicolas Sarkozy[1] especially regarding road traffic. Speeding controls have become more systematic thanks to a widespread network of radars. Some respondents believed that since radars take photos (cars registration number) this could be interpreted as an erosion of one's privacy.

  - According to respondents, September 11th only had a noticeable impact when travelling by plane, even more when travelling to the USA: more controls in Airports (body searches, luggage searches) and stronger presence of Policemen.

[1] Secretary of State for the Home Department between the years 2002 and 2004.

- As for the role of the media, it was thought to increase the feeling that privacy is more and more eroded:
  - Respondents had mainly heard about cases regarding the downloading of MP3 files and measures taken by the music industry to protect their works. In fact, the first trial in France of a young man who downloaded music files for his personal use occurred in December 2004. Respondents (+ younger) were very worried about this issue which was perceived by most as an infringement on privacy. They stated that consequently they had become more prudent when downloading files and tended now to keep this activity secret.
  - Others mentioned that the media regularly alludes to telephone tapings made by the Police or illicit actions of web hackers.
  - Some (a minority) also declared that the media had recently mentioned the project of secured identity documents.

- ***Personal experiences and concerns:***

- While all respondents believed that there is less privacy today, they expressed different levels of concern about it.

  - In fact, for the majority, the loss of privacy is rather a concern. It is a topic they are used to speaking about with relatives-friends-colleagues, especially regarding the impact of the Internet on privacy (e.g. exchange of tips regarding ways to avoid Internet drawbacks).

    "I feel that we are spied on the Internet"

  - For a minority (about 1 or 2 people in each group), the diminution of privacy was not experienced as a problem:
    - ✓ Some had a **"naïve"** behaviour and tended to believe that their personal data was not interesting enough to be used by a third party. For instance, regarding telemarketing calls, these respondents tended to believe that phone calls were made at random.
    - ✓ Others had a more **"pragmatic"** behaviour and believed that giving personal information is part of the Internet rules: as soon as one uses the Internet he/she accepts to be tracked because the advantages provided by the Internet are worth being tracked.

*"I don't feel concerned, who would like to steal and use my identity?
I'm not interesting enough!"*

*"I think that telemarketers call me because I have a funny name…
I presume they choose a district or a street by accident"*

*"It's fair, I want to purchase, they want to sell… these are trade rules,
I want to be informed, I accept to have my data collected…"*

- For most respondents, the salient concerns regarding privacy invasions were related to day-to-day life and the workplace:

  - **Day-to-day life**:
    - ✓ **Internet:** respondents declared they were fed up with the invasions of SPAMS and pop ups. Also, some (+ youngest and males respondents) knew that any web user can be tracked thanks to the IP address and were aware of the presence of cookies that monitor browsing habits.
    - ✓ **Telemarketing:** for some, being disturbed at home by telemarketers was considered as a stronger intrusion in private life than SPAMS (which can be thrown away without even reading them). Most respondents felt that telemarketing calls were more and more targeted.
    - ✓ **Mobile phones:** some respondents deplored the recent usage of SMS sent by phones providers to propose commercial offers. Others also pint pointed the fact that, if needed, Police could monitor and track the movements of a mobile user.
    - ✓ **Credit card:** some respondents thought that their purchase habits could be tracked through their credit card.
    - ✓ **Credit information:** credit files were perceived as an importance source of personal data, renowned for being exchanged between consumer credit companies. For some, the requirement of the medical history when asking for a credit was perceived as a privacy aggression.
    - ✓ **Surveillance cameras:** some spontaneously spoke of the development of the presence of cameras in big cities as an infringement on privacy.

"As soon as you purchase something over the Internet,
you are bombarded with SPAMS from the competitive websites "

"If Cetelem does not grant you a consumer credit, Cofinoga will know it right away!"

  - **On the workplace**:
    - ✓ **ID badges:** these badges are used in some companies to come in/out, some respondents thought they could also be used to monitor workers time of arrival and departure.
    - ✓ **Computer activities:** respondents believed that computer scientists in their company could know the types of programs used and websites visited, by who, when and how often. The awareness of this kind of monitoring was stronger for those working through a computing network (e.g. in banks).

"I feel as if I was working with someone looking over my back"

- The other ways in which their privacy could be compromised were related to the increasing use of cards with computer chip implants:

  - **The Parisian public transport card, called "Navigo"[2],** is renowned to be able to record commuters' trips for a certain period of time. As a consequence, some "Navigo" users expressed fears about the use of these data and the monitoring of their daily schedules/comings and goings (horary, places, length of transport etc.).

  - **The French Health Insurance card, called "Carte Vitale"[3],** presently records the members' name, surname, birth date and Health Insurance identification number. Some respondents explained that this card will also soon record each member's medical history and raised fears about it.

  - **All kind of loyalty cards** with a computer chip implant were thought to be able to track consumers' purchase habits and to enable targeted mailings and telemarketing.

- In the end, a minority of respondents indicated that they had encountered a real "aggression" of their privacy. Only one respondent in Group 2 (Consumers & Citizens) explained he had experienced a fraudulent use of his credit card when purchasing in a supermarket.

- When probed on whether certain groups in society are more susceptible to invasions of privacy than others, opinions were divided. Respondents especially thought of commercial invasions and felt that as everybody is a potential consumer, everybody can potentially be tracked. Others believed that people with little knowledge about commercial practises (especially lower income groups) could be more vulnerable than others.

[2] A personalised (it mentions the user name, surname, birth date, address and has a digital photo) yearly public transport card in use since 2001 in the Parisian area.

[3] A card deployed as of 1998 and owned by French insured persons aged 16 and above to justify that they are members of the Health Insurance system. With this card, each member can claim reimbursement of their health expenses.

- ***Protecting personal privacy***

- A large number of respondents declared to take action to protect their privacy while using the Internet as well as their fixed or mobile phones:

  - Regarding the Internet:
    - ✓ Using a pseudo, a false identity, providing wrong / false personal data (an action however more difficult if there is a need to deliver goods).
    - ✓ Using secured websites, firewalls, anti-bugs, anti-SPAMS, anti-cookies.
    - ✓ Blocking pop-ups (an action proposed by some monitor researcher such as Google).
    - ✓ Classifying some email addresses as "unwanted".
    - ✓ Unsubscribe from a web newsletter.
    - ✓ Never "check" the policy which says *"I accept that my personal information be used for mailings, phone calls and commercial emails".*
    - ✓ On the work place, automatic deletion of the websites visited.

  - Regarding fixed and mobile telephones:
    - ✓ In order to avoid telemarketers phone calls, some respondents explained they had asked France Telecom to be registered on the "red list" (i.e. a telephone directory that cannot be communicated or exchanged). Others observed that since they had subscribed to one of the new competitive providers (such as Free, Alice) they were not bothered by telemarketers, certainly because directories have not been edited or exchanged yet.
    - ✓ Some respondents explained they had deactivated (on their phone) the visual recognition of their telephone number in order to prevent people from reading it and using it for commercial purposes.

- There was in fact a common feeling that one needs to be resourceful and needs to develop one's own technological "DIY" in order to protect one's privacy. Respondents declared that tips are the most often exchanged through word of mouth between relatives-friends-colleagues. Indeed, information regarding privacy protection was felt difficult to find. In case of a serious invasion of their privacy, respondents stated that they would ask for information and assistance to the following institutions:
  - The C.N.I.L "Commission Nationale de l'Informatique et des Libertés" (this institution is more developed and explained in the "Legislation" chapter page 17).
  - The Ministry of Justice or the Ombudsman ("Médiateur de la République).
  - Consumers associations and magazines such as "Que Choisir" or "60 millions de consommateurs".

II. Expectations regarding privacy issues in the future

- In the 5 – 10 up coming years, the majority of respondents foresee an exponential invasion of their privacy. They explained this prediction mostly through two factors:
  - The permanent evolution of computer-based technology and the Internet.
  - The constant growth of the market for personal information, which was imagined to become even more "greedy" in the coming years: thought to require more and more personal data, create more and more data bases and exchange files on a worldwide scale.

    "For the coming years we expect a kind of 'snow-ball effect',
    I cannot imagine how the situation could be better"
    "I imagine to be a bar code, we'll become more and more paranoid"

- A minority of respondents (+ among the "pragmatic" ones) considered this increasing invasion of privacy as a commercial progress and declared to prefer to be appropriately targeted by companies.

  "Great, I prefer to be addressed appropriate offers"

- Some others were optimistic (+ among the "naïve" respondents). They predicted a moment in which all data would be eventually collected by companies and expected a "saturation" effect which would decrease the monetary value of files. Some others also imagined a "lassitude" behaviour in regards to the usage of the Internet and predicted that in the future it will be less interesting to track people via that kind of media.

  "Companies already know everything about you…
  what kind of information could they need in the future??"

- Examples of the ways in which things may not be as private in the future included:
  - **Incomes:** incomes are a taboo in France. Wages are in fact considered as private information, which is not communicated even between relatives or friends. However, as some politicians and chairmen began to reveal how much they earn, some respondents expected to see that kind of information becoming "public" in the future.
  - **Health data:** the "Carte Vitale" (the French Health Insurance card) will soon record each member's medical history. Some respondents disagreed with the idea of collecting this kind of personal information and feared an illicit usage of their medical data.

- **Police records:** the French Police records trace all penal sentences into 3 different certificates, which are more or less exhaustive depending on the recipient (the citizen itself, an administration, judicial authorities). At present, those certificates are highly protected. For instance, if an administration wants to obtain information about a potential recruit, it can only have access to one type of certificate (the less exhaustive). Some respondents feared that, in the future, it would be possible for anyone to have access to the certificate which records all the sentences.

- One of the biggest threats expressed by respondents for the coming years was about the crossing of administrative data (such as marital status, number of children, medical history, incomes…) with purchasing data. "Citizens" respondents (Group 2) were less pessimistic. They all already had used the Internet to contact a national administration such as the Treasury (for instance to fill-in the income tax form) and stated that they strongly relied on the administration to protect their privacy.

- Finally, another important threat expressed for the future referred to the divulgation of "intimate" data such as sexual behaviours (heterosexual or homosexual), politic opinion, and religious denomination.

III. Privacy: technologies and legislation

- ***Technology***

- As already stated, respondents perceived an inevitable greater usage of technology in the future.

- Most of them expressed little confidence about computer-based technology in their daily life, either at home or at work. Indeed, technological innovations were felt too fast to be understood and followed. The Internet was considered as an unreliable technology, vulnerable (cf. hackers) and beyond human control.

"Certain people are able to infiltrate the CIA !"

"Technology advances too fast, there are constant new discoveries which you cannot keep up with"

- Most respondents acknowledged that they did not have enough nor explicit information to know how computer-based technology might affect their personal privacy. Most stated that they learn how to protect themselves through word of mouth between relatives-friends-colleagues.

*"We can imagine that our banker knows everything that we consume, so maybe one day he will say: you should not go to Courchevel * ?? " (* high end skiing station)*

"When there is a scandal we learn ourselves, we document ourselves"

- As for means to protect privacy while on the Internet see parts "Protecting personal privacy" (page 13) and "Privacy issues: consumers" (page 25).

- ***Legislation***

- We observed a rather good knowledge and awareness of the French legal framework.

- In fact, most respondents were able to quote either the French laws relative to privacy or the institution which controls the edition and the exchange of computer data bases (the CNIL).

- Respondents globally showed confidence that such laws would be effective at protecting their privacy. However, they all required more information and communication about them.

"What exactly does the CNIL? I would like to hear more about its actions"

- **The law "1978, relative à l'informatique, aux fichiers et aux libertés"** (law about computing, files and freedom/privacy). Respondents rarely named that law with that exact terminology. They rather spoke of "Loi Informatique et Liberté" (Law about Computing and Freedom/Privacy). This law was even spontaneously mentioned by some in the self-completion questionnaire at the very beginning of the group (see Table 2). Respondents described that law as *"a legal framework which protects our personal information".*
  - ✓ One respondent explained that he mentioned that law once during a telemarketing phone call, to ask to be cancelled from the telemarketer's files.
  - ✓ Some others remembered to have recently received an email from different websites (especially e-commerce websites) asking if they could continue sending emails/newsletters.[4]

- **The CNIL "Commission Nationale de l'Informatique et des Libertés"** (National Commission about Computing and Freedom/Privacy). More than half of the respondents in each group knew that French institution by name. However, most of these persons could not give details about its role and functions. Only one or two persons per group (often those who had dealt with computing files for their work) could do so. These persons explained that the CNIL was in charge of controlling the respect/application of 1978's law. In that context, each company who plans to store personal data needs to declare its intention to the CNIL and ask for an agreement. From the citizens side, anybody who believes to have suffered from an aggression of his/her privacy can complain to the CNIL.

- Respondents also mentioned laws about **"intellectual property" (copyrights)** and the **"right of publicity".**

[4] This measure follows from the 1978's privacy law. Websites were forced to send an "authorisation request" to all their web users before December 22nd 2004, otherwise they would be penalised by the CNIL.

- **As for a legal framework for companies:** when probed about laws that place restrictions on how companies use personal information, respondents assumed that such a legal framework exists in France, without being really aware of its roles and functions. For instance, some thought that some details recorded on Curriculum Vitae (age, marital status, nationality…) as well as administrative information (wage, number of children, medical history…) were confidential and could not be exchanged between companies. In case of an infringement of their professional privacy, the CNIL did not came out spontaneously. Instead, respondents declared they would resort to professional legal institutions that defend workers rights such as "Work Inspection" (Inspection du Travail) and "Conciliation board" (Prud'Hommes).

  "I presume that laws exist for companies, but they are very discrete…"

- **As for a European legal framework:** when probed about European privacy laws that place strict restrictions on how governments use personal information (including restrictions on the sharing of personal information), the majority of respondents had never heard of such a European legal framework. While some assumed that CEE had elaborated specific laws, others believed that privacy was not a European preoccupation and sarcastically declared CEE was more interested in establishing agriculture and agri-food rules…

  "CEE is more concerned about the percentage of cocoa in chocolate
  and about our snails grading than privacy laws…"

- **Security versus Privacy:** most respondents agreed that some measures aimed at increasing security were most often at the expense of privacy.
  - A vast majority of respondents (+ among females who especially fear physical and sexual aggressions) felt that as far as safety is concerned security measures are justified. Some considered these measures as being part of the evolution of our society. Many thought that they were efficient measures and spoke of the diminution of aggressions or traffic accidents.
  - However, others (a minority) believed that measures such as surveillance cameras in cities strongly compromise their privacy and evoked fears of political / illicit usage of the images.

  "I accept to be filmed if the streets are more secure" (Female)

  "My privacy is not compromised with cameras, I am not bothered, I do not feel monitored" (Female)

- **Security versus Privacy in the future:** a majority of respondents expect that in the future the emphasis will be more on “security” than on “personal privacy”. This prediction was thought to depend closely on politic elections, the increase of security measures being inevitable with a conservative government.
  - A majority again accepted this coming evolution well and thought it was important to live in a secure environment.
  - A minority expressed their sadness towards this evolution and could not accept to see their personal privacy infringed upon. They declared that if this prediction became effective, they would certainly develop “opposition” behaviours.

“This evolution will depend on the next government, these are political measures, if Sarkozy is elected we will for sure have more cameras in the streets”

IV. Privacy issues: workers

- Most of respondents declared to be monitored on the work place:
  - Internet usage: time spent online, websites visited, emails sent or received.
  - Telephone usage (mostly phone calls to mobiles).
  - Productivity through ID badges and the connection to the company network.

- Respondents agreed that while they are on company time they are working and thus not dealing with private affairs. Privacy in the workplace was only related to personal data such as income and administrative data.

  "As soon as you are working, private life remains at home"
  "We all know that we are not really authorised to use the Internet for personal use"

- However, we draw the attention to the need to take into account the social control which operates during focus groups. The presence, in each group, of managers / ex managers certainly lead to a rather good acceptance of monitoring, while in reality French people claim their right to act freely.

  "As an employer, I am authorised to see what kind of websites you visit" (Manager)
  "In my company, I had decided to bann the phone calls to mobiles, after that my bill was reduced by 30%!" (ex Manager)

- We observed a good acceptance of monitoring in the workplace (productivity, the Internet and telephone use) provided that employees were made aware of these practices and the consequences.
  - For instance, some respondents knew that their phone calls were recorded and checked each month, others explained that they knew that computer scientists were monitoring the websites employees visit.
  - Others stated that monitoring was rather implicit in their company, information was most often given by word of mouth and rumours between colleagues.

  "I know that we are permanently monitored while we are surfing the Internet"
  "I was told that someone was requested to stop calling mobiles during his/her work hours"
  "I hope that my company does not use the data collected in my ID card with bad intentions"

- Some declared that companies should be supple, and should consider their employees as “responsible adults” who would not compromise their job for Internet matters. In that context, monitoring should depend on the moments and the frequency: surfing websites for personal use during breaks should be accepted versus doing so frequently during working hours. One respondent, in charge of managing a team, believed that taking into account everyone’s private life (personality, hobbies etc.) was a good way to trigger motivation. Thus, each of his subordinates was informed that he/she can spend a certain amount of time online for private use and deals whenever he/she had the time to do so.

- Respondents shared the idea that companies should monitor all their employees equally. Some respondents evoked L’Oréal offices where it is said that the banning of sending emails from private email boxes (such as Yahoo) concerns everyone in the company. Monitoring only one group of people would be otherwise perceived as a kind of segregation between employees, or would infer only negative purposes (employees dismissal).

V. Privacy issues: travellers

- Respondents acknowledged that travelling can somehow compromises privacy: body and luggage search, passing through the X Ray gate, filling-in of immigration forms were thought to be actions at the expense of privacy. These situations were felt to concern more air travelling (in France as well as abroad) than railway travelling.

  "Opening my luggage and searching my panties really bothers me!" (female)

  "I hate to fill-in the American immigration form, I usually write false information"

- In the post September 11th context, the perception of tighter border control was prevalent among most respondents. Some who had recently travelled to USA spoke of deeper body search (taking off clothes and shoes) and long queuing. However, some thought that the USA had always practised tough controls in comparison with other countries.

- We observed little knowledge about the American government requiring advance travel information from the French government. Few respondents mentioned *"a new Passport"* with detailed data but without being able to say more about it.

- Respondents were consequently given an explanation of the requirements from the USA of documents with biometrical identifiers: digital image of face, finger print or eye iris.
  - Some first perceived that requirement as a revenge from the American government regarding French opposition to participate in the war in Iraq.
  - Others, among "pragmatic" respondents, could not perceive a change as the French current Identity Card is already secured with a fingerprint. Most thought that the French current Identity Card was more practical than the previous paper one (because smaller and more resistant). In addition, these respondents tended to feel that being searched was a more important infringement on personal privacy than providing a photo or a fingerprint.
  - "Naïve" respondents did not feel bothered by that requirement, wondering who could care for their identity.
  - Some others reacted negatively to this American requirement and perceived it as a strong infringement on their privacy.

    "I think that Americans would be more interested in my acts than in my identity, I do not mind showing my photo and my finger print" (Naïve)

    "When I hear that I want to support Cuba!" (Anti)

- When probed about tracking the movements of French citizens by the French government when they exit/re-enter their country, respondents thought this measure was already implemented. Again, opinions were divided between “pro” and “anti” (cf. Privacy versus Security pages 18-19) :
  - This kind of security measure did not bother the “pro security” who felt that it is necessary to control and eradicate terrorism.
  - However it bothered the “anti” who perceived it as a strong infringement of their privacy.

VI. Privacy issues: consumers

- ***Loyalty programs:***

- Few respondents (about two per group) declared to participate in a customer loyalty program such as Airmiles. These respondents were all members of the Air France program, called "Fréquence Plus". Only one respondent had both "Fréquence Plus" and "American Express" cards [5].

- When probed on why they participate to such Airmiles loyalty programs, all respondents evoked the attractiveness of the rewards (i.e. miles).

- All had a precise idea of the purpose of these programs (i.e. gain consumers' loyalty). However, we noted less familiarity with what the company can do with the information it collects, and even a kind of indifference mostly justified again by the attractiveness of the reward.

  "Perhaps they know and record the places where I use it to travelling…
  but I do not care, it's the game, in the end I win free travels…"

- The only person who used both "Air France" and "American Express" was satisfied with the statutory privilege offered by Amex and also with its practicability (insurances and worldwide network).
  - However, she did not know that her purchase habits could be monitored through the Amex card and that her "purchasing behaviour" could be sold to other companies participating in that program.
  - Neither did she remember having been asked to give her consent about the use of her personal data and stated not having received targeted commercial offers yet.
  - When the process was explained to her, she accepted the idea of seeing her "purchasing behaviour" sold to other companies. Indeed, she assumed that they would certainly be reliable companies – like American Express – which will fit her needs.

[5] The "Fréquence Plus" card is not a credit card, it enables each member of Air France loyalty program to capitalise miles each time she/he travels, miles which are then converted in free trips. However, it is possible to capitalise more miles if using the American Express card.

- ***Purchasing over the Internet:***

- Nearly all respondents had already made a purchase over the Internet. The purchases they spontaneously mentioned mostly referred to cultural goods (books, discs, DVD, shows…), transports (railway, airway) and hobbies (photo cameras…).

- The reasons for purchasing over the Internet were the possibility of finding good prices and the convenience (ease of use, delivery at home, short times of delivery).

- However, all evoked concerns with regards to safety while purchasing over the Internet:
  - In order to minimise the risks of identity thieves (credit card number), respondents declared to purchase only on e-commerce websites of renowned and established companies.
  - Some stated that the presence of the padlock pictogram (meaning secured pages) reassured them, while others thought it did not prove anything about security.
  - Some however asserted that they preferred to do only research over the Internet (e.g. for transports, shows) and then tended to book and pay by giving the credit card number by phone. In fact, these persons thought that the phone was more secure than the Internet as only one person was speaking over the phone instead of millions over the Internet.
  - Nobody had heard about the "e-credit card" recently implemented in France by some banks.

"I trust the well-known company names because I know that they have good insurances in case of safety problems"

- In France, you can read that kind of policy on websites: "*Conformément à la loi Informatique et Liberté n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, vous pouvez exercer votre droit d'accès et de rectification sur vos données nominatives en cliquant sur la rubrique xx".* Two respondents (out the 4 "Consumers" in Group 2) declared to read the privacy policies on websites and considered them as useful and adequate measures of privacy protection.

- Some also explained that in order to protect their privacy while purchasing over the Internet they had different email addresses, one being only dedicated to purchase. In that way, only the "purchasing" email address was invaded by SPAMS and commercial offers.

VII. Privacy issues: citizens

- As already stated, respondents had all noticed that in recent years, surveillance cameras have become much more commonplace.

- They were all able to give examples of where cameras are being used today and for what purpose: monitor potential criminal activities and guarantee citizens' security.

- Respondents spoke of cameras placed in:
  - The work place (surveillance cameras in the entry/exit),
  - The streets for traffic regulation,
  - Transports (Airports, inside buses-subways-trains, in the station itself and on the platforms),
  - Parking,
  - Banks and ATM,
  - Department stores, shops and supermarkets,
  - Public administrations and Ministries,
  - Some bar toilets (to prevent the presence of junkies).

- As already noted (c.f. Privacy versus Security page 18) this issue received divided opinions among respondents:
  - The use of surveillance cameras was seen as acceptable and justified by a majority. These respondents did not perceive that measure as a real intrusion of their privacy. Indeed, since these cameras are most often not visible, they are rather deemed as a reassuring and imperceptible (nearly virtual) presence. These respondents assumed that cameras were operated by Police or by municipalities.
  - However, a minority considered those security measures as an invasion of privacy and raised doubts about who really operates them. They evoked fears about a political / illicit usage of the recorded images and questioned the existence of a legal framework for surveillance cameras.

"Everybody criticises speed radars although now people drive much more carefully" (pro)

"We live with them, we do not think about them" (Pro)

"Who is behind the cameras? For what purpose are they used? It makes me think of Moscow's eye and Pravda…" (Anti)

- Then respondents were specifically probed on the usage of surveillance cameras in public places. They were told that there are approximately 150 000 surveillance cameras operating in London, providing surveillance of almost the entire city:
  - The majority of respondents saw it as an effective way to prevent aggressions (+ females who especially fear physical and sexual aggressions). Some had heard of a girl raped in London and saved thanks to the cameras. The example of the city of Levallois-Perret[6] was also quoted in each group as a good illustration of the efficiency of surveillance cameras in public places.
  - Although the same "anti" minority was opposed, basing their objections on privacy protection but also on the ineffectiveness of these measures at reducing criminality.

" I would feel more comfortable with cameras, in case of aggression I would be glad to receive help. A girl has recently been raped in a train near Paris and Police has found her aggressors thanks to the cameras" (Female)

"Everybody knows that there is less criminality in Levallois-Perret since the municipality has implemented cameras on each street" (Pro)

"How can a camera prevent aggressions?! Mr Sarkozy speaks of an 'insecurity feeling' in France and takes security measures, however violence has never been so rampant as today!" (Anti)

- Finally, respondents were probed about the widespread introduction of surveillance cameras in Paris. Some believed that cameras were already implemented in Parisian streets (even if less widespread than in London) for traffic regulation. Others wondered if these cameras were already used for security purposes. Again, this issue received mixed reactions between respondents:
  - A majority accepted this idea for its perceived gain of security.
  - A minority rejected that project and felt that in such a context Paris would become an unpleasant place to live.

"In Paris, the Police Prefecture can already follow a car from downtown to the suburb with its cameras"

"I can watch people in the street, people can watch me, thus I do not see the problem of surveillance cameras in the street…" (Pro)

"Cameras would become part of the landscape like little birds?! I would consider it as an infringement of my privacy, it would mean no more private life, I would feel good only at home, I leave Paris right away if they do that!" (Anti)

[6] A town in the western and wealthy suburb of Paris, famous for its widespread use of surveillance cameras.

VIII. Ranking of different types of privacy(*)

In the final section of the focus groups, respondents were asked to fulfil a self-completion questionnaire (see Appendix B) that was designed to rate four types of privacy, both in terms of the level of importance in protecting each type and the degree to which each type of privacy is under threat today.

(*) given the nature of qualitative research and the limited target we interviewed, these findings should not be interpreted as statistically representative.

The findings summarised in Table 3 show the following trends:

- ***Ranking of importance for the four types of privacy:***

Generally speaking, we note that while in Group 1 the ranking was rather homogeneous (i.e. few differences between the items), in Group 2 the differences between the items were more marked.

Across the two groups, three types of privacy were assigned by at least one respondent as the most important to maintain: "Communication", "Information" and "Territorial".

- "Territorial" privacy received the largest number of "most important" ratings.
- "Bodily" privacy was never assigned as being the most important.

- ***Ranking for the four types of privacy under threat:***

Across the two groups, the four types of privacy were assigned by at least one respondent as the most under threat:

- "Information" privacy received the largest number of "most under threat" ratings.
- "Territorial" privacy received the largest number of "least under threat" ratings, just followed by "Bodily" privacy.

Table 3
Ranking of different types of privacy

Group	First Name	Age	Gender	Profile	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)			
					Bodily	Communication	Information	Territorial	Bodily	Communication	Information	Territorial
G1	Jérôme	25	Male	Traveller	4	3	2	1	3	1	2	4
	Jean-Louis	60	Male	Traveller	2	3	4	1	3	2	1	4
	Marie-Agnès	47	Female	Traveller	2	1	3	4	1	2	4	3
	Melody	23	Female	Traveller	3	1	2	4	3	1	2	4
	François	40	Male	Worker	3	2	1	4	3	4	1	2
	Virginie	28	Female	Worker	4	3	2	1	1	3	2	4
	Daniel	55	Male	Worker	3	4	2	1	4	2	1	3
	Lola	53	Female	Worker	4	3	2	1	2	4	3	1
				Total	25	20	18	17	20	19	16	25
				Average	2,5	2	1,8	1,7	2	1,9	1,6	2,5

Group	First Name	Age	Gender	Profile	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)			
					Bodily	Communication	Information	Territorial	Bodily	Communication	Information	Territorial
G2	Olivier	30	Male	Citizen	4	3	2	1	2	1	3	4
	Christophe	28	Male	Citizen	4	2	1	3	2	4	1	3
	Guy	58	Male	Citizen	4	2	3	1	1	2	3	4
	Leila	36	Female	Citizen	4	3	2	1	3	4	1	2
	Aline	20	Female	Citizen	4	1	3	2	2	3	1	4
	David	33	Male	Consumer	2	4	3	1	4	3	1	2
	Linda	49	Female	Consumer	4	1	3	2	4	1	3	2
	Annick	55	Female	Consumer	3	4	1	2	4	2	1	3
	Bernard	47	Male	Consumer	4	3	2	1	4	1	2	3
				Total	33	23	20	14	26	21	16	27
				Average	3,3	2,3	2	1,4	2,6	2,1	1,6	2,7

4. Conclusions

The findings from the two Parisian focus groups pointed-out a number of conclusions:

- In the majority of respondents' minds, there is less privacy nowadays and there are plenty of potential threats of infringement. Computer based-technology and the Internet were seen as the main "enemy", both incontrollable and opaque skills which can work against privacy.

- Respondents shared the idea that little information is available on how to protect ones privacy (especially on the Internet), a context which explains the strength of word of mouth between people.

- We also observed two behaviours among a minority of respondents for whom the loss of privacy is not a concern: "naïve" people that do not really realise the commercial interest of their personal data and "pragmatic" people who have decided to live with that situation and even to take advantage of it.

- However, we noted that respondents had no real experience of privacy infringement. Maybe because the French legal framework works well? In fact, respondents were reassured by the presence – even if vague – of the CNIL and the 1978's law.

- As for "privacy versus security", this issue was perceived as being closely linked to politic decisions. We observed that, among the groups we interviewed, a vast majority prefers to put its privacy aside when security is concerned. Consequently, the presence of surveillance cameras was globally well accepted by these respondents. Although, a minority systematically criticised the idea of increasing security at the expense of privacy.

- In the future, respondents expect that privacy will be become more and more at stake as technology advances. Their strongest threat referred to the crossing of administrative data with purchasing data. Respondents also feared an infringement of their privacy via the divulgation of "intimate" data. Some were more optimistic and thought they would develop the typical Latin behaviour of "countering the system".

5. Appendixes

APPENDIX A

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.

- 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?**

o **Have you ever experienced a serious invasion of privacy?**

– What kind of invasion of privacy was it?

o **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?

o **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].

o **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 mn)

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 privacy laws that place strict restrictions on how 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 Travellers (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 France track the movements of its citizens as they exit or re-enter France? 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 France 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 France 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, 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 Paris 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!

APPENDIX B

Self-completion Questionnaire (in French)

QUESTIONNAIRE SUR LA PROTECTION DE LA VIE PRIVEE

Prénom : ________________________ Groupe n° ____

Certains experts de la « protection de la vie privée » parlent de quatre domaines de la vie privée : l'image, la communication, les données personnelles, et l'intimité.

Dans un premier temps, nous vous demanderons de classer ces différents domaines de la vie privée, selon l'importance que vous accordez à la protection de chacun d'entre eux [merci de bien vouloir classer ces différents domaines de 1 à 4 : en n°1 ce qui est le plus important pour vous et en n° 4 ce qui est le moins important pour vous].

L'image ex. être regardé(e) ou surveillé(e) sans votre permission ou sans que vous en soyez informé(e)

La communication ex. quelqu'un écoute vos conversations ou lit vos emails sans votre permission ou sans que vous en soyez informé(e)

Les données personnelles ex. le contrôle de l'information qui est collectée à votre sujet

L'intimité ex. ne pas être dérangé(e) chez soi, pouvoir avoir des moments où l'on est totalement seul(e), loin de qui que ce soit

Et à présent, pourriez-vous classer ces mêmes domaines selon le degré de menace que vous estimez peser sur chacun d'entre eux ? [merci de bien vouloir les classer de 1 à 4, n°1 pour le domaine qui vous semble aujourd'hui le plus menacé, n°4 pour le domaine qui vous semble aujourd'hui le moins menacé].

L 'image ex. être regardé(e) ou surveillé(e) sans votre permission ou sans que vous en soyez informé(e)

La communication ex. quelqu'un écoute vos conversations ou lit vos emails sans votre permission ou sans que vous en soyez informé(e)

Les données personnelles ex. le contrôle de l'information qui est collectée à votre sujet

L'intimité ex. ne pas être dérangé(e) chez soi, pouvoir avoir des moments où l'on est totalement seul(e), loin de qui que ce soit

APPENDIX C

Demographic profile of group participants
(based on collected recruit screener data)

Group 1

Profile	First Name	Age	Gender	Position and branch of industry
Traveller	Jérôme	25	Male	Manager (Outdoor centre)
Traveller	Jean-Louis	60	Male	Retired - Ex Manager (Logistics)
Traveller	Marie-Agnès	47	Female	Secretary (Medical)
Traveller	Melody	23	Female	Biochemistry student (Thesis)
Worker	François	40	Male	Drawer (Building Trade)
Worker	Virginie	28	Female	Accounting manager (Bank)
Worker	Daniel	55	Male	Juridical adviser (Practice)
Worker	Lola	53	Female	Executive saleswoman (Software)

Group 2

Profile	First Name	Age	Gender	Position and branch of industry
Citizen	Olivier	30	Male	Engineer (Computers)
Citizen	Christophe	28	Male	Development manager (Automation)
Citizen	Guy	58	Male	Retired - Executive (Computers)
Citizen	Leila	36	Female	Accounting assistant (Industrial pumps)
Citizen	Aline	20	Female	Business student (Business School)
Consumer	David	33	Male	Store manager (All terrain bicycle)
Consumer	Linda	49	Female	Sales representative (Estate agency)
Consumer	Annick	55	Female	Agency director (Temp agency)
Consumer	Bernard	47	Male	Administrative officer (Professional training)