

**EKOS Test Group I – May 3, 2004 5:30 – 7:30 p.m.
Toronto**

Moderator: ... at the end of this when we get into, get into a regular portion in black and white. That being said, everything is kept confidential. When we actually go to the reporting stage and write up our reports, we don't identify any individuals. We may say men versus women, you know, young versus old, Toronto versus Montreal, you know, those kind of differences. In terms of tonight, hopefully very easy going. There are no right answers tonight, there are no wrong answers. It's also okay to disagree, so if Nicolai says one thing and you disagree, Paul, we need to sort of hear ... because some of the issues we'll talk about, there are differences of opinion. And, it's also okay to change your mind, if you've heard and you have one view, you hear somebody else's arguments, it's okay to say, "You know what, I think I can accept that."

I basically have three roles as a moderator. One, I raise issues for discussion, I may not always answer your questions as for me, but I may put it back to you and say, what does that mean to you, Elwin, I want to see how it's interpreted. I also sort of play traffic cop to be sure that everybody has a chance to speak and that no one person sort of dominates. And as I always say, my third and my most important role is to keep track of time. We've asked you hear from 5:30 to 7:30 and I'm sure you want to be done on time. Any questions so far?

Can we go around the table introduce yourself by your first name only and say a little bit about your background: what you do ...

Nicolai: My name is Nicolai. I'm working for a transportation company, big trucks, trailer trucks, you know. And myself, I'm involved in accounting and administration. I say administration because sometimes when the lines are busy I'm also supposed to answer the phone and if somebody wants to place an order to assist or if somebody has any complaint or would like quotes for some jobs, I am the person who do that.

Moderator: So you do everything.

Nicolai: [laughs] It's a small company.

Antonia: My name is Antonia and I work for a pharmaceutical company and I'm a recent graduate from the University of Toronto.

Moderator: And doing what?

Antonia: I work in the pharmacy.

Moderator: Okay.

Audrey: I'm Audrey. I'm an interior designer. After 20 years of working for a furniture manufacturer I'm on my own and I'm also doing research in offices, office design.

Corey: My name's Corey. I'm account manager for retail sales and I've applied for my MBA for next year, so just waiting to hear for that from that.

Moderator: Good.

Jay: My name is Jay. I'm working at IT and security in a bank. And I try to take care of hackers and stuff like that.

June: My name is June and I work for a law firm. I'm an administrator at the law firm and I sort of am office manager as well. Our people travel a lot so I keep things running when everybody's out of town.

Ellen: My name's Ellen and I'm a nurse and I work in a telehealth environment and I'm team leader there. And I've been in nursing in a whole bunch of settings over the years, whether its community or education, hospital setting or whatever.

Moderator: Okay.

Paul: Hi, my name's Paul and I'm assistant editor of Dan Diamond and Associates we do, we're a publishing company we do the *NHL Guide and Record Book*, *Total Hockey*, *Total NHL*, Blue Jays books and things like that.

[Side comment and laughter.]

Moderator: Okay, you all have a pen and paper in front of you. Can you just write "Toronto 5:30" at the top. I'm going to collect all the paper at the end.

When you hear the word privacy, what's the first thing that comes to mind? And I want you to write it down. So no right answer here, no wrong answer. Privacy. What's the first thing that comes to mind? [Pause] First thing that pops into your mind. Everybody have something?

Nicolai: One word only?

Moderator: Or whatever comes into your mind. Privacy. And when you hear the word security, what is the first thing that comes to mind. I want you to write it down.

Corey: Do you want us to write down words you mention, too, or is it ...

Moderator: Yes. So the first one is privacy, and the second one's security. The first thing that comes to mind. Paul, what did you write for privacy?

Paul: Secrecy.

Moderator: Secrecy.

Paul: I don't know why, that's the first thing that came to my mind, okay? So I put it down. You know, privacy, things that are told just to one person by another person are private and they should be kept secret from anybody else.

Moderator: Okay. Ellen?

Ellen: Confidentiality.

Moderator: Confidentiality. June?

June: Legislation.

Moderator: Legislation. Jay?

Jay: My responsibility.

Moderator: My responsibility.

Corey: Internet.

Audrey: Control over environment.

Moderator: Control over environment.

Antonia: Personal.

Nicolai: I have confidentiality and something very discrete.

Moderator: Something very discrete. Okay. Reverse. Security. What did you write?

Nicolai: Stability.

Moderator: Stability.

Antonia: Safety.

Moderator: Safety. Security guard.

Antonia: And security guard.

Moderator: That's okay.

Audrey: Shut unwanted out.

Moderator: Shut unwanted out.

Corey: I wrote home and alive.

Moderator: Home, alive.

Jay: Hard to reach.

Moderator: Hard to reach.

June: Person regulating entrance to a building.

Moderator: Person regulating entrance to a building.

Ellen: Computers.

Moderator: Computers.

Paul: I put money.

Moderator: You put money.

Paul: Security – money is security.

Moderator: Meaning what?

Paul: Meaning, if you have enough money you're secure.

Moderator: Okay, gotcha. Gotcha. Okay. A whole host of different things. Well, we're going to talk about privacy tonight, a little bit about security. And go a number of ways. But often people talk about privacy as a value. What is a value? What does that mean to you? What is a value?

MP: A value is something each individual should have, or something. And privacy is a value that should be had by each individual to a certain degree.

Moderator: Okay.

FP: Something that you would maybe judge, like a set of criteria or something like that that you are judging against.

Moderator: Okay.

Jay: My idea is explain to the panel that people that we want that privacy want that information [inaudible word].

Moderator: Okay. What is a value?

FP: A positive asset.

Moderator: A positive asset? What do you mean?

FP: It's a good asset.

Moderator: Okay.

FP: Something good to have.

Paul: Also it could be a good moral value, you could have certain moral values that certain things are, as far as you're concerned, are socially acceptable, and other things are not.

Moderator: Like what?

Paul: Swearing in a public place? Does that make any sense?

Moderator: Okay.

Corey: I think it's something that's fundamental to each individual. Like equality, accountability.

Moderator: Equality, accountability.

Corey: Fairness.

Moderator: Fairness. Okay.

Ellen: Something that I would hold dear and sort of helps set the stage for ethical behaviour for me.

Moderator: Okay, so I've got here freedom, equality, what was that?

Corey: Accountability.

Moderator: Accountability, so kind of high level value. What do you think when someone says, well, privacy is a value. Does that make sense.

FP: Mmmhmm.

Corey: Yeah, privacy's about each individual. Each individual has a certain amount or privacy that they would value obviously.

Moderator: Antonia, what do you think?

Antonia: Well, I think values are something that are important to you, so privacy is important for everyone.

Moderator: Okay.

Nicolai: Yes, I support all of this opinion as an asset, something having not only rights, to use another word, but also it makes sense and it's very important, let's say it this way.

Moderator: Okay. Jay?

Jay: It depends, the privacy it varies from person to person, so people think that something's more valuable, it's more important to be private, you know.

Moderator: Okay. One of the things, I mean, my company does is we both focus groups, but we also survey. We just survey right across the country. And a lot of those surveys we often ask questions about privacy, and whether or not they feel they have less privacy in their daily life than they did five years ago. How would you answer that question?

Paul: I think that's true, yeah.

Moderator: You think it's true?

Ellen: I think it's true.

June: Definitely true.

Corey: I would say no. There's less tactics out there to invade your privacy. Like I know my friend's office, he's on camera all the time and his boss can watch him over the Internet all the time.

Moderator: So you would agree that you have less.

Corey: Yeah.

Moderator: Okay. Audrey, you're shaking your head.

Audrey: Five years ago I had the same, I had just as little privacy five years ago – ten years ago! I think five years ago it's the same as it is now.

Moderator: Okay. Antonia?

Antonia: I think I have more privacy now, considering I'm older now [general laughter].

Nicolai: I think the situation is the same as before.

Moderator: Okay. Why – I've got all three. I've got less, more, the same. Those who say less, Paul – you five. Why? Why do you have less privacy today?

Ellen: Maybe we're becoming more aware of the fact that more surveillance is being employed. For instance, even just the basics, like going through traffic lights and things like that, there are cameras for everything now and you're aware more of surveillance in the workplace as well, that sort of thing, monitoring everything. So I think it's just, maybe just it's more sort of you're aware of it kind of thing.

June: I think sort of as an addendum to that, I think there's different types of ways it's increased. Sort of the visual type of things, with cameras type of stuff. But also every time we do any transaction with any credit card or any bank card, or we're on the security, we're on the Internet and, you know, we're leaving

a trail behind us. So that we're less secure, I think, therefore we have less privacy than we did have before.

Moderator: Okay. Paul?

Paul: I think there's less privacy because of the Internet and stuff like that and because of all the government actions and stuff like, we have put a certain number in the bank, or like even if we go through a stop light, as you said, the cops can get an impression of your license number and get a whole bunch of data on what traffic offenses we've done in the past year and stuff like that and things like that.

Moderator: And you said and what governments have done. What do you mean by that?

Paul: Well, just like if we put our Social Insurance Number and you can just like put it into a computer or something, and then all of a sudden other information comes up regarding the individual, like their health or age, and things like that.

Moderator: Okay. Jay.

Jay: I think that the industry is realizing the importance of information provided by people, so like the businesses instead of growing vertically, are growing horizontally to different kinds. For example, now a bank can provide more services if they know what are the habits of the people and what are their preferences. So they pile databases with information that they can get from their client. So also databases are being sold from one company to another. We get spam because we put an email address on website "X", and those websites collect email addresses and they give them, but they also provide information with the preferences, what websites I visited. I would not have these concerns more private or depending on what ..

Moderator: Okay. Corey?

Corey: I just think that there's more ways, like, I would say to survey where you've been going or what you've been doing. First of all, like the technology's a lot better than it was five years ago, so there's greater paper trails out there of you, like Big Brother's watching everything we do.

Moderator: Okay. Audrey said no different.

Audrey: I think five years is too short a time to spend. Maybe I'm wrong, but that's just my perception.

Moderator: No wrong answers here. What would be different, if five years is too short, you said ten years?

Audrey: Ten years ago, then I would agree, but my perception's the same.

Moderator: Why?

Audrey: Because five years ago I *perceived* that I was monitored with all my transactions and everything I did just as much as I am now.

Moderator: Okay. So what's changed – use ten years ago. What's different?

Audrey: Well, ten years ago I don't think that I was as aware. I didn't use the bank card, I didn't have – I wasn't aware of my Visa being tracked the way it was, I'm constantly getting calls now that my Visa's been compromised, so it's sort of I've been made more aware.

Moderator: So for you it's just a time frame issue.

Audrey: Yes.

Moderator: Okay. What do you mean your Visa's been compromised? What do you mean?

Audrey: I have bad luck with my Visa. I don't know, people get my number. And they call me before I even know anything's happened. So obviously, they've got great tracking systems.

Moderator: Okay. Antonia, you said more. Why?

Antonia: Well, like on a more personal level the whole, you know, my family stuff, there's more privacy than five years ago.

Moderator: Because they don't know as much?

Antonia: Yeah, more independent.

Moderator: Okay, so your frame of reference is you're more independent, you do things now.

Antonia: I'm out longer.

Moderator: You stay out more, which they don't need to know about.

Antonia: Yeah.

Moderator: Okay.

Nicolai: Maybe I'm the only one who says the same. I basing on that the info behind every one of us is the same as before. We cannot say that it is completely different. The carriers of the info are changed, but the situation is the same. Ten years ago, who has the right to check, to make a background check on you, can access that info, and that's the same info. Now, somebody else who is not authorized may access some part of the info because of our own mistake. That's why I say it's the same. If we don't make a mistake, nobody will get more info in order to jeopardize your existence using whatever, the other colleagues, participants in this survey said, getting card number or whatever document, they cannot obtain it to do something. It depends on us, how we handle our personal security. So, on the basis that I mentioned, it's the same, for me. There is no change. We have privacy, I say.

Moderator: Okay. Ellen?

Ellen: I was just thinking that I think there's more ways to compromise our security now because, for instance if we're talking about governments, there are larger databases, especially now if we're talking about some larger company databases and that type of thing. We know that folks can always hack in, or whatever, there's always attempts to do that. And, so that there are specific types of information that I don't mind people knowing what I do, but there's other types of information that I really want to be mine, and not to have anybody aware of. But I think the fact that there is more data in many different banks now than there ever was makes us much more vulnerable to some degree.

Moderator: Okay. So I've got a mix of views on the table in terms of less, about the same, more. Put that aside, how concerned are you actually about your privacy today? Have you ever talked about it, and discussed it? We're in a room today talking about privacy, but how concerned are you? Paul.

Paul: I'm not really too concerned about it.

Moderator: Not really too concerned.

Paul: About privacy? No.

Moderator: Ellen?

Ellen: Still don't use the bank card. I'll use my Visa, but never use a bank card. I never caught on to that type of thing.

Moderator: Why?

Ellen: It's another trail, I use credit cards, but I also pay cash for a lot of things.

Moderator: Okay. June, how concerned are you?

June: Not too concerned, I just find that some things more of a nuisance than anything. Because, I think sometimes it's trial and error. When you get, when you're doing things, for instance, especially on the Internet, sometimes you fill out information on the Internet the purposes that you think is for your own purpose, but you forget that the other side is using that information for their purposes as well. For instance, with things like spamming or having communications that you're not really interested in receiving, that's not something that you think you're inviting, but in fact through trial and error maybe you find out that, yes, you are sort of inviting these kinds of things and that's something that you find out through experience.

Moderator: But that's not really concern, that's more of a nuisance?

June: Yeah.

Moderator: Okay. Jay, how concerned?

Jay: I am very concerned about privacy.

Moderator: Why?

Jay: I find that my information, I don't want my information to be spread around or like people using my information, so I try to hide the information that I can. Because I think that the privacy is my responsibility and is how so they keep out.

Moderator: So you just mean your personal information or what?

Jay: No no I'm saying that my personal information can be used. I know it can be used and I don't trust systems that I don't know.

Moderator: Okay.

Jay: So if I don't know how my Visa account going to be used or if I don't trust the company just to give ...

Moderator: Okay. Corey.

Corey: I guess, are we talking specifically Internet related or ...

Moderator: No, just are you concerned about your privacy today?

Corey: Not really. I guess I more work in an open office concept, so in our little quad, so I don't really have too much privacy. I guess there are other – if I wanted to be private I could go to a separate room, so. I don't have that much to hide.

Moderator: June.

June: I'm marginally concerned.

Moderator: Marginally concerned.

June: Since I started doing Internet banking.

Moderator: Okay. Antonia.

Antonia: Well, I'm a little concerned about Internet, like I don't like to give my information out, I like to – prefer to use cash than my debit card, but that's about it.

Moderator: Okay.

Nicolai: I'll say I'm not concerned at all, because when I have any doubts I think before I do something, and if I'm not sure that something will affect me, I won't do that. For example, if they said purchasing something over the Internet, I don't use that at all, because it's not secure that only the company I purchase from, only the company can use that. So ...

Moderator: Okay. And that's your bid on that. What kinds of other things do people do to protect your privacy? So I've heard pay with cash, I don't keep stuff on the Internet. What else do you do? Can you actually think of anything you've done in the past six months, year, that you've done to protect your privacy?

Audrey: The baggage tag. You know the little luggage tag? Now that I'm self-employed, I don't have a sort of non-descript business card to put on my baggage tag, so it's like, okay what phone number do I put there, I don't want to put my name and phone number on a baggage tag that's going who knows where. So that ...

Moderator: Okay, that's an example. Anything else?

Ellen: I got a new, not Norton anti-virus, but I got some new sort of software for my computer.

Moderator: Okay, new software. Anybody else?

Jay: I use fake emails when I have to reach certain places.

Moderator: Okay, fake emails.

Antonia: Yeah, me too.

Corey: I worry sometimes that the phone lines are going to cross or something, so I use my cell phone versus my landline to make the call.

Moderator: Okay. Anything else?

Nicolai: Maybe never expose very important info, like birthday or Social Security Number in the Internet, you know. Just of the kind this way, you know, to you personally.

Ellen: I bought a home shredder.

Moderator: You bought a home shredder? Who else?

June [?]: I bought one.

Corey: What, shredding papers?

Moderator: When did you? What prompted you to buy a shredder?

Ellen: All the discussion in relation to identity theft within the last six months or so, and I was trying to cull some stuff out and I thought, well, I don't want to just put this down, because you never know where it's going to end up.

Moderator: Okay.

Corey: When I post my PIN, I always put my hand over to cover my PIN number.

Moderator: Okay. We've kind of got a little bit of info into how, you've talked about the last five years. Have any of your attitudes changed in the past five years? Anything different, anything more to add?

Paul: You mean, about privacy, security?

Moderator: Privacy. What about since September 11th? Anything different? Yes?

Nicolai: I am a little bit afraid, if you have to travel, my plane, you know? All the time thinking about, you know, some of the people inside might be involved in something like that.

Moderator: Okay, anything different?

Ellen: I don't like the idea that somebody's noting my movements back and forth across the, you know, you just have your courses through the country, or back and forth over different countries and that type of thing. And I feel like that that's an invasion of privacy. You know, before you used to sort of go where you wanted to and you felt sort of free to do that. And now you feel that there really is a Big Brother. I sound paranoid, I know it, but I mean it's just all those things became much more focused I think.

Moderator: Since September 11th. Anybody else? Anything you've seen in the media change your attitudes? Ellen, you had talked about identity theft and it prompted you to go out and buy a shredder. Anything else you've seen in the media about privacy that's changed your outlook?

Nicolai: Just recently about the identity theft, they show a documentary – a person who stole those bank cards and went to Calgary or Edmonton probably and then they start to draw money from the accounts, something like that it was.

Moderator: Okay. Ellen?

Ellen: I was just going to say there's been a whole lot of legislation on confidentiality and privacy and personal information, and a couple of acts in Ontario and stuff that applies sort of federally over the last year and I suppose it's been aware because it's affected us and in my workplace. You know, the activities it has to do with.

Moderator: Okay. I heard Ellen say the word a serious invasion of privacy. Can I see a show of hands. Who has ever experienced a serious invasion of privacy? Corey. Anybody else? What was it, can you say?

Corey: At York University the bookstore they had a camera installed over where you bought the books, and people were duplicating your debit cards because they say you enter your PIN number in and were withdrawing from your account. I believe over 200 people.

Nicolai: You lost money?

Corey: But I got it back, it was withdrawn.

Moderator: Okay, that's an invasion. Anybody else?

FP: It's not along the same lines, it's just, being broken into. I think that's pretty serious. I had my wallet stolen with your information in it. That's another thing, too.

Moderator: Okay, anybody else?

Jay: Maybe missing mail, it's not good. You know, it's nothing, but still, you don't feel good when somebody's stealing mail.

Moderator: Okay, so that happens to you?

Jay: Yeah, it's happened.

Moderator: Anybody else?

Ellen: I had my wallet stolen.

Moderator: Wallet stolen.

Antonia: I had my mom read my diary.

[Laughter.]

Moderator: Well, can you give me some other examples of privacy invasions.

Audrey: Going through the airport ...

Moderator: And?

Ellen: Having, going through the sort of the process with the automatic checks and that type of thing and going through your luggage and that type of thing. You know you don't have anything there, but that seems like an invasion when they're like your private things and personal things.

MP (Corey/Paul): But they only do that because they don't know. Basically, you have to have really good security.

Moderator: Okay. What are some examples of invasions in your day to day lives?

Paul: Spam.

Moderator: Okay. What else?

Ellen: Unwanted mail.

Moderator: Unwanted mail. Audrey?

Audrey: I was thinking invasion of your personal space, some get, people get too close, and that happens in a crowded subway, crowded line-ups.

Moderator: Okay, people getting too close. What else?

MP: Telemarketers.

Moderator: Telemarketers, okay. What other types of invasions, privacy invasions in your day to day lives?

June: There's monitoring of email at the office.

Moderator: Monitoring of email at the office.

MP (Corey/Paul): People reading over your shoulder, your email.

Moderator: Okay, anything else.

Ellen: Some of the quality monitoring procedures that we have in place at work where our calls are monitored.

Moderator: What about an invasion by government? Some examples.

Jay: [?]

Moderator: Pardon?

Jay: [?]. There is this concept that there is in the background of the Internet is over this. So the major communication between countries has over the background in the United States [?]. So there is this eyes, activities of intelligence that is looking for key words in the communication that it is passing. Whether it's encrypted, or autoencrypted, part of the information. So for that reason there was [?], that is how it is called. So the IT people to, like kind of protest against this, had to send zillions of emails with key words so the system crashed. I don't know if it happened, and I don't know if it's really true. And I think it increased the need for security.

Moderator: Can anyone give some other examples of possible privacy invasions by the government?

Audrey: Monitoring public places?

Moderator: Monitoring public places.

Audrey: Cameras and such.

Moderator: Okay.

Ellen: I sometimes wonder when I sign a petition. Who gets this in the end, and what do they do with it? Is it just going to the MPP I'm sending it to, the MP? I just wonder about that.

Moderator: Okay. Corey?

Corey: I can't think of it.

Moderator: About governments?

Ellen: A friend of mine's active in a couple of different sort of movements and her concern has always been about cameras, police taking pictures and things at different events. But the one thing that bothers me is whether or not data is really kept private between big silos of government, where is it not supposed to share between. So you come down – data's not supposed to be shared, health data's not supposed to be shared, but you wonder what does go across.

Moderator: Okay.

Antonia: For me it's the security of the privacy is that your government has all this information and I don't trust them to be secure about it.

Moderator: Okay. What about invasions by companies?

Nicolai: One example will be advertising something that is not any value, but they advertise on purpose in order to sell.

Moderator: Okay. How does that compromise an individual's privacy?

Nicolai: Okay, you don't want your time to be spent stopping some program and invading your space this way, entering this info, you don't believe and you don't want that. Maybe 70% true, but according to me, it's not like that.

Moderator: Okay. Other examples of invasions by companies.

Jay: Some parts of the, like when they are advertising their product on, I don't know, line of credit or a product, they check if they have databases with other people and how they can say, okay, I'm going to send this email with offering this all of the people that decided to arrange between this and this, or they have teams or they, so they have a type of file of client, so they can contact a person directly, whether they are able to pay or is going to be a good client. So I think that all that information, it's sometimes too much information.

Moderator: Okay. What about in the workplace?

June [?]: Well, some employers like monitor your phone calls and your email, your Internet, all that's an invasion.

Moderator: Anybody disagree? You're in the workplace, should employers be allowed to monitor phone calls? Should they be allowed to monitor ...

Paul: What types of calls are you having. If the policy is that you're not supposed to take personal calls, then sure. If you're not allowed to take personal calls and stuff like that, they should be allowed to monitor your phone calls.

Corey: That's your alternative, you know, if you want to make a personal call, then it can be monitored. Go to another room, or tell someone that you're making a personal call.

Moderator: June.

June: I was just sitting here wondering, well, does every company have the resource to monitor every single phone call or are you pinpointing certain maybe problem areas that's used as sort of a problem-solving device. But of course then, outside of the workplace, for instance when you call a bank or something like that, they often tell you we're going to monitor this for your protection, so there's that type of phone call as well, that sort of monitoring that's done. I'm not sure it's for our protection. I'm sure the bank is paying for it, so I'm sure it's for their protection, but.

Moderator: Okay. In the workplace: should employers be allowed to monitor your phone calls? Yes or no?

Nicolai: Only when it's for training purpose. I've heard sales people, they make phone calls over the phone and the manager or the person who is in charge to train that person listen to see how the person develops skills, because he's supposed to hear the other party also.

Moderator: Antonia?

Antonia: No.

Moderator: No? Why not?

Antonia: I don't know, I just don't think it's right. Because I know my work wanted to start doing that and, but they didn't, so.

Moderator: Audrey.

Audrey: It doesn't bother me. I use my cell phone if I want to make a personal call.

Corey: I think it depends on the type of work you do.

Moderator: Meaning?

Corey: Like for the bank example that was given before, or if you're working something on the phone, you want to be able to I guess, keep a trail of what you're doing. I don't know an example is, I have, like when you sign up for a credit card, just like that, they always record that call. So the type of work that you do, the call should be recorded, just for legal purposes or protection purposes.

Moderator: Okay.

Jay: I think they shouldn't be doing it. Like, they hire some person is because they are mature enough to do what they are doing, but in some cases it, like I don't know, my friend, I'm pretty sure that he was being monitored. People that are in key places may need to be monitored, because we are all human and ...

Moderator: Okay, I'm going to come back to this issue a little bit later. Any other ways that you can think about why privacy could be compromised? I've heard identity theft, I've heard credit information, surveillance cameras, tracking your purchases, I've heard all that so far. Anything else?

Jay: Movement?

Moderator: Tracking of movement?

Jay: Like when I've been ready to fly. I don't know ... friends?

Moderator: Friends?

Paul: How would your friends be able to be tracked?

Jay: Well, it's not that but you always read in the news that they capture this person that was really with this other person, that was really in with this other person, so they make all the chains of people, I don't know how they do it.

Moderator: Now, speaking more generally, are there some groups in society that are more susceptible to invasions of privacy than others?

Corey: Maybe the affluent?

Moderator: The affluent?

Corey: Yeah, people want their money? Or the information ...

Moderator: Audrey, you're shaking your head.

Audrey: But they don't – they can afford the locks to prevent that.

Moderator: Okay.

Antonia: I think famous people.

Moderator: Famous people?

Nicolai: We've come to the conclusion that as high as you are in society, the more concerned you are because some people may use that info against you, so these people I believe are very concerned.

Moderator: Okay, so either famous or rich. Others?

MP (Jay/Nicolai): Politics.

Moderator: Politics.

FP: Since 9/11, you know, accusations are made to certain groups and profiled, that's a lot of unwanted attention and definitely an invasion of privacy. So there's no choice now...

Ellen: Visible minorities.

Moderator: Okay, visible minorities, ethnic groups.

FP: Vocal people.

Moderator: Vocal people, what do you mean by that?

FP: People who have opinions and state them.

Moderator: Okay. What other groups? Why do you say that?

FP: Just some of the activists you see over time and, it's just, I have the perception.

Moderator: So how would they have less privacy?

FP: People want to know who they are, what motivates them.

Moderator: Okay.

FP: Undue attention, they draw attention.

Moderator: Who else? Who else may be more susceptible? Corey said rich people, and Audrey shook her head no. Where do the rest of you come down on? Do rich people have less privacy?

Paul: I think they have more privacy. They have access to better security, they would be far better off, far more privacy, really.

Moderator: Ellen.

Ellen: They're probably more likely to be targets of invasion if they happen to be somebody that somebody particularly wants to know about, you know, anybody in the public eye for whatever reason I think is a potential, potentially could have their security violated.

FP: Maybe privilege allows you to rebuff this, though, it attracts it, but it may allow you to more effectively rebuff some of that unwanted attention.

Moderator: But do you think that rich people have less privacy?

FP: Greater privacy.

Moderator: Greater.

MP: You say they're more susceptible.

Corey: No, they're more susceptible, but they also have the bigger barriers.

Moderator: Nobody said low income groups. Why? So their there for the rich, for the famous people, activists, ethnic minorities, visible minorities, nobody said low income groups. Are they any different from any other group in society?

Nicolai: Maybe the interest.

Moderator: Pardon?

Nicolai: The interest is not equal to these people compared to the others.

Moderator: Okay.

Ellen: Economics.

Moderator: Meaning what?

Audrey: Well, there's no purchasing power, I mean less of a marketing interest, no sales interest. Or, not no sales interest, but a different sales interest, maybe a different approach.

Ellen: But it's interesting that you bring that up, because they often are more susceptible to government interference because they have to fill out government forms to do, you know, to go to the bathroom, so to speak. Their lives are ruled by government regulations, it's awful when you think about it.

Moderator: Okay, so you're making a private/public sector distinction.

Ellen: Yeah.

Moderator: Okay, any other groups? What about the sort of, what about looking forward? You personally: how likely is it you actually will experience a serious invasion of your personal privacy over the next five years? You personally. Do you think it's likely, Paul?

Paul: I don't really think so. No.

Moderator: No.

Nicolai: Maybe in the future there will be more possibilities to be checked directly from, let's say, Revenue Agency of Canada. Now we fill out our tax returns and nobody comes to see, let me see your documents.

Moderator: Do you expect more?

Nicolai: Yes, because maybe people will be involved in more machinery, or ...

Moderator: So you can see it happening. Antonia?

Antonia: No, not really.

Moderator: No. Ellen?

Ellen: On a sort of gut level, probably no.

Moderator: Audrey?

Audrey: I think yes.

Moderator: June?

June: I think no, I think it will be more creeping. I don't think it will be a big invasion of privacy.

Moderator: Corey?

Corey: I say yes. I think there will be more opportunity five years from now.

Moderator: Okay. Jay?

Jay: More invasion.

Moderator: Why do you say more creeping, June?

June: I don't expect to have a sudden invasion of privacy. I expect it, that things will just creep along kind of thing, I don't expect it to be sudden. I think that more and more there's a little bit more.

Moderator: What could you see happening?

June; I don't know if I see anything in particular happening, maybe honestly I don't know.

Moderator: Okay. Audrey? What can you see happening?

Audrey: I just see more and more monitoring of our wired world. People, they know what we watch on TV, whether we're satellite or cable, our .. in other words in our wired world, and wireless world, it's just, I think there's more opportunity for surveillance. With the technology.

Moderator: Pardon?

Audrey: The technology.

Moderator: Technology.

Audrey: Becomes better and better all the time, every year it's a bit better.

Moderator: So where do you see the creeping happening?

June: Well, from that, in terms of maybe there can be other ways of perhaps new ways will be developed of getting more information? A little bit more, a little bit more, maybe ways that maybe we don't realize at first, but then that's, the information comes out kind of thing.

Moderator: Okay.

Nicolai: I believe in two major directions: mass fingerprinting taken, and DNA banks, probably will be, or maybe.

Moderator: Okay. Mass fingerprinting, DNA. Next. Jay?

Jay: Yeah, definitely, the databases are becoming closer and your profile is getting more defined. So in the future is not going to be, a bank is going to be able to check all your preferences, all your what you

want. And I think that they comprehensive relation to power and they drag together all the information they can, this is possible.

Moderator: Okay. Audrey?

Audrey: I'm just laughing, because we'll microchip ourselves like we do our dogs now.

[Laughter]

Nicolai: Who knows.

Moderator: What about, I mean, Jay talked about preferences. In the future, what do you think will be less private in your lives. So they'll know more about preferences, they'll know more about that you like this brand and not this brand.

Nicolai: Yes, I can say in the near future, it's not possible still to read the minds, so that will be impossible so far, and let's say twenty years from now I don't believe it will be possible.

Moderator: Okay. You talked about DNA, fingerprinting. Forward-looking. Ellen.

Ellen: No, I was just thinking about sort of DNA printing brings up the whole issue of national identity cards, that really is sort of putting your privacy at risk, those type of things.

Moderator: In what way?

Ellen: I want my information to be my information, I don't want to have to carry around a card that everybody ... it's the same as health information. Do we want to have a card that has all our health information it so everybody can key it in for some information that's really positive, but there are other things that I think are sort of debatable, i.e., any sort of mental health issues, those are things that you may or many not want to have on those types of things.

Moderator: Okay.

Ellen: So I think those types of things would create a lot of discussion, because that really is invading your privacy.

Moderator: Okay. If I asked you sort of for different things in terms of that could affect your privacy. If I asked you to pick one thing, what would you say is the biggest threat to your privacy in the future? I want you to write it down. The biggest threat to your privacy in the future. [Pause] And why. [Pause] So if you pick one thing, the biggest threat to your privacy in the future. Corey?

Corey: I was just saying people are, will be able to take my banking information again.

Moderator: Okay, so financial related.

Corey: Yeah.

Moderator: Audrey?

Audrey: For me it's technological surveillance.

Moderator: Meaning what?

Audrey: Technology, they'll be able to – Big Brother will be watching. They'll know whether I drove the car, where I took it and how I took it.

Moderator: Okay.

Audrey: Everything. Whether I locked the door on the house.

Moderator: Okay. Five years away, ten years away, fifteen?

Audrey: I'd say ten years, only from a financial standpoint. From a technological standpoint I'd say we're there, like with GPS and everything.

Moderator: Okay. Antonia.

Antonia: One thing I think of is just like with those cards, all those points cards and credit cards.

Moderator: Okay, so knowing everything about what you buy.

Antonia: Shopping patterns.

Moderator: Biggest threat.

Nicolai: For me, if they create big banks for DNA info, it is possible for big players, because we are not computers, we are not perfect, big players can plant that info to cover, to sacrifice some ordinary person to cover, so it's very dangerous, because DNA is the biggest, you know, proof that somebody's done something. These are the trace nobody can control to such extent, not to leave any trace. So anytime it will be something like that on the crime scene. And the masters of that field, sometimes they are working for the evil. Many, many cases, many – look at the books, you can see. And that's, I think, it's very dangerous.

Moderator: Paul?

Paul: I said the same thing as Corey did, bank card or Visa card, they can keep track of your financial transactions using that can sort of establish what your buying patterns are.

Moderator: Okay.

Ellen: Health information can be used in a lot of ways by folks, i.e., insurance companies, to permit or deny some benefits or claims, those types of things, so based on where you are in your life now.

Moderator: Okay, so knowing too much about your health information. June?

June: I think technology and the way technology continues to grow, and in the uses to which that can be put, or uses and misuses. For instance, with the health card or with a national identity card, you plant that with a certain kind of chip that has so much information in there, but if those can be made, they can also be duplicated, but they can be stolen or something like that, it's a huge, it's a risk if you're carrying something like that around, it has everything about you.

Moderator: Okay. Jay?

Jay: I think if my Visa, for example, Visa card, any person can impersonate you and use that information to do transactions.

Moderator: Okay, so kind of identity theft on the financial side. Okay. Let me see a show of hands. Who uses the Internet? At work? Okay, most of you. I mean, how much do you rely on technology in your lives?

FP: Too much.

Moderator: Too much?

Ellen: Significantly at work.

Moderator: Significantly at work.

Ellen: Whether it's computer or telephone, and at home, I'm on every day.

Moderator: Anyone else?

Corey: I haven't been to the library in the past five years.

Moderator: Okay, so Internet, computers, cell phone I've heard. What else?

Corey: For research.

Moderator: What other technologies?

Ellen: Videoconferencing.

Moderator: Videoconferencing.

June: There's palms and all the handheld devices.

Moderator: Handheld devices. How confident would you say you are in terms of, do you know how technology, you all use the Internet every day, you all use your cell phones ... how confident are you in terms of your knowledge of how technology might affect your privacy? I'll ask you last ... The Internet.

June: I found out really through trial and error, because, you may fill in some information and you realize it can come back to bite you later in terms of spamming, you know those types of things that can be a real nuisance.

Moderator: Okay.

Corey: I think with online purchasing, I always look for sites that have, that are secure sites, like Paypal or whatever or not.

Moderator: How do you know if that's secure or not?

Corey: Because of the lock at the bottom of the screen.

Moderator: And what does that mean?

Corey: It's secure. [Laughter]

Moderator: But what makes it secure? What does secure actually mean?

Corey: I don't know, that someone's encrypting my credit card information and no one can take it.

Moderator: I don't mean to put you on the spot, I'm not a tekkie either, I can't pretend to know the answer, but what does that mean to you, that it's encrypted and ...

Corey: I guess that it's a secure site, that only me and whoever the merchant is has my information, no one else has the opportunity to capture that information.

Moderator: Okay. Others. June, when you're going online, do you know how it works, or do you know what's possible?

June: I expected to be hacked, and I'm just – I have no faith in the security of the Internet. I figure, if it happens, it happens.

Moderator: Okay.

Corey: And you're protected, too, if something happens. I mean, when I got my money taken out of the bank, like you're protected from that, the banks and credit cards have a protection policy in place, so I'm not too worried about it.

Moderator: Okay.

Corey: It's an inconvenience, but ...

Moderator: Inconvenience? Ellen.

Ellen: I see the systems that we have in place at work in terms of sort of fire walls and blocks and encryption when we sort of send or receive messages to specific folks. So hopefully those are some of the tools, the best that they have at the moment, to actually sort of have the information go securely. The only thing that's as good as security is to have somebody else try to break it, because then you can always kick it up an extra level.

Moderator: Okay, let me see a show of hands: who says you have enough information to know how technology might affect your privacy. You know. Let me see a show of hands. Okay, one of you knows, and you do it for a living. Well, how – let me ask you then. How do you see the Internet affecting your privacy.

Jay: The Internet definitely affect your privacy. It's all online, and if you have the knowledge, you can get the information you want.

Moderator: What can you get?

Jay: I don't know, if I'm able to reach Audrey's computer at home, I can get all her information, I can look in all the temporary files and see what has she browsed, and maybe I can get the Visa card information in some of the pages. I don't know, I can get preferences, I can get, I can get her to spam for me.

Moderator: Okay. What are some – who's actually ever done anything in terms of trying to protect their privacy while on the Internet? What do you do? I mean, I heard Jay earlier say you give fake email.

Nicolai: What I did, as I mentioned, personal info is dangerous in one way to have. So if they say open an email account and put your birthday, don't put your exact birthday in order to open an account, you don't need to state exactly your personal info, put something different. And you get the account. I mean, email account, not other account. So, I'm sure that if somebody get that info, it won't be used, because it's not my personal info. And the gentleman, I'm sorry, Corey, your name, Paypal is secure because the person you purchase with doesn't know your bank account because they send the money to them as an email saying that that person purchased the item, so they, Paypal, takes the money from your account and transfer to their account, so the other party cannot know your account number. And I believe, 99% in the security of Paypal because they'll not lose that profitable business making it very simple and mistake to lose their clients. If something happened, nobody would go through them. But can you kill the package with the golden egg? Never, you'll do your best, so.

Moderator: Okay. What else have people done to protect their privacy on the Internet?

June: Put on a firewall, or some kind of protective software to try and weed out some of the stuff.

Moderator: Who has access at home? Okay. And Ellen said that she, you bought software.

Ellen: Yeah, I've bought MacAfee, and I've got virus protection and I still do dial-up, so I never have it plugged in to the, I always just plug it in if I'm going to, so.

Moderator: Who's taken any steps at home to protect their home PC? Yes, yes, no? How come?

Jay: I don't know, I don't do, I don't have that much private information on my PC at home. I'm, the thing is, if I put too much control my PC connects and says alarm, alarm, so I make more break for performance than security in that case.

Moderator: Okay. Audrey?

Audrey: I have software, but what about these alarms that are coming in then? I mean they just crash your computer?

Jay: I don't have many in, they're just so old that they don't even work.

Moderator: Okay. What about how governments are using technology? What's different today in terms of what they do, how they use it?

Corey: I think it's a lot more efficient today, government technology. Makes transactions go a lot quicker, like you can go to the mall now and get your, like renew your drivers license there instead of waiting in line for like an hour, an hour and a half.

Moderator: Okay.

Corey: The governments definitely are more efficient now. More cost effective, too.

Moderator: Okay, so you use it to improve service. What else.

June: It helps you with your taxes, too. You can put your information in quickly and get it all done kind of things, using a different, various methods to do that.

Moderator: Okay. Paul.

Paul: You know I agree with what she was saying, you know, do your income tax and all sorts of different things.

Moderator: Okay. What about sort of what about, what things exist to protect your privacy today? What laws exist? Are there any? Don't know?

Nicolai: I don't know.

Moderator: Don't know? Antonia? Don't know?

Jay: I think there is, people base on one of the first basic laws, but I'm not sure which one.

Moderator: June?

June: I don't know specifics, but I know there is for instance like consumer protection laws, which, I presume have some privacy built in there, but I don't know the exact details.

Moderator: Skip Ellen for a second. Paul?

Paul: I don't really know.

Moderator: Ellen, do you know?

Ellen: There is federal protection in relation to confidentiality and privacy that went into effect this year, so that everybody has to, every company has to sort of disclose if they want our information or whatever with you. So most of them have privacy disclosures on them now. There's also a new health privacy act that has just passed the provincial legislature and we also have a privacy commissioner in Ontario who is responsible for looking after privacy and does report to, does at least have a sort of yearly or a semiannually report to the legislature.

Moderator: Okay, well, there are laws that exist on sort of the federal side that place strict restrictions on how federal governments or their departments use personal information and what they can do, and putting restrictions on sharing personal information. So, you give all your income stuff to Revenue Canada or CCRA or whatever, you give other types of information to HRDC if you're dealing with your pension or your Employment Insurance, and there's laws sort of that govern what they can do and what they can't do with personal information. So none of you were really out, Ellen mentioned. When you hear that there are laws that restrict government departments can do. Does that, do you believe it?

[End of Side 1]

Moderator: ... that they're ineffective? Paul?

Paul: What were you saying? About certain ...

Moderator: They basically put limits on ... you give your information to Revenue Canada. There's restrictions on what they can do with your information, and things what they can do and can't do. Likewise, if you're unemployed, then you –

Paul: Do you mean like spreading information to other departments and stuff?

Moderator: Or actually what they can just do with that information. Like there's restrictions. There's privacy laws that say that they can do this, but they can't do that.

Paul: I don't believe they probably, no.

Moderator: Why.

Paul: I just have my doubts that things are, they may as well pass things from one section to another section within the government and things like that.

Moderator: Did you know there's laws in place?

Paul: I did not know that, no.

Moderator: But why, when you hear there's laws, do you still say, I have my doubts.

Paul: Well, there's individuals in each of those departments that could like, sort of, break the laws a little to their advantage and stuff like that.

Moderator: Okay. Others?

Antonia: Well, I don't know, how would we know? Like if there, like we would never know if they're not, if they're actually sharing our information with other departments.

Moderator: But if there's laws in place, do you think they would follow. Let me see a show of hands. Who thinks there's laws in place that restricts what federal governments can do with your personal information? Let me see a show of hands – who has confidence that the federal government would follow its own laws when it comes to...?

FP: Who has confidence in the federal government?

[Laughter]

Moderator: Do you make that distinction? I mean, there's the federal government sort of manages the economy, but federal government to follow its own laws in terms of privacy, personal information?

Jay: May I say something?

Moderator: Of course.

Jay: People have doubts because they experience many weaknesses. But in general, without laws, we cannot reach that level as a human society it's improved so far. So, in general I say, the law, yes, I believe it of our system.

Moderator: But do you think that ...

Jay: Yes, I believe it.

Moderator: So you think that if there's a law in place the federal government will follow its own laws.

Jay: Yes, I believe that.

Moderator: Antonia?

Antonia: I don't think so, because I think that there's something else that the government has with all our information on it. Not, all the information we have from all the different departments, you know, Revenue Canada, Transportation, anything, is all together in one, you know, database.

Moderator: Okay, so yes, no. Audrey?

Audrey: I think they could, but not knowing what the laws might be and how many loopholes there are available to them for the sharing of information among departments, I mean, it depends on what the law is and how it's structured that if it's structured loosely enough, then yes, they can follow it.

Moderator: No, there are strict guidelines in terms of what governments can, the feds can do, and what they can't do. And so in some cases it's very strict, in other cases this is permitted, by legislation. Do you think that they'll follow their own legislation? No. Why?

June: No. I think that information goes through too many hands, and past too many eyes. Whether it's, I don't know whether it's intentional or not, I just don't know, I don't have faith in the government.

Moderator: Okay. Corey?

Corey: I think they do. It's a very procedural body or organization and I'm sure that there's penalties or repercussions if they don't follow the laws.

Moderator: Okay.

Corey: So I guess there's a sense that they have to follow the law or face the consequences.

Moderator: Okay.

Jay: If we go back to the original point if we think that we are being affected, privacy in our workplace, I think that's a case that will, where we will want that we will be monitored and seeing what people that work in the federal government will do with our information, so we will want a place to see that that information is not being shared, it's keeping private.

Moderator: But do you think that they will follow their laws?

Jay: I think if those checks are in place, I think they are followed.

Moderator: And do you think the checks are in place?

Jay: I think to make sure that things are kept private, I think they have to keep those checks in place.

Moderator: June.

June: I think laws are established to establish standards. I don't think standards are always adhered to. You shoot for the top, but I don't think you always quite make it and otherwise, we wouldn't really have too many scandals.

Moderator: Okay, so do you have confidence that they would follow their own laws? No. Ellen?

Ellen: I'd like to have confidence that they would. I think there's too many ways that it can, whenever there are people involved, data can be, things can be manipulated. So I think now that there are, I think that with balances in place, you need somebody who's really on it, you need somebody who's going to bring things forward and I'd like to think that they will.

Moderator: But do you have confidence?

Ellen: No.

Moderator: And you. Paul?

Paul: Yes.

Moderator: Ellen, you don't have confidence, but what's your confidence right now? What is it?

Ellen: I guess on two levels. If you have a database of information, there's always going to be somebody saying I want this. So there's always a personal level. The second level I think probably, what's been happening with the federal government lately, in relation to the scandal that's gone on, in relation to the how money was distributed. And it sort of, that raised a flag in relation to either what checks and balances are there or are we acting ethically if something does come up, and taking action to either remedy or deal with it.

Moderator: Okay.

Ellen: I guess that's why.

Moderator: Okay. So we've got a lot leaning no, some leaning yes. What else do you think affects the scandals. What happens if it's the Ontario government? Do your views change any?

Corey: I think the government's the government no matter what level.

Moderator: The government's the government no matter what level. June?

June: Yes, I wouldn't feel any differently between the federal government and the Ontario government.

Moderator: Okay, Ellen?

Ellen: Same.

Moderator: Same?

Paul: Same.

Moderator: Same. Well, okay, so that's – there is legislation that government, what government departments can do. As of January 1st, 2004, there's also privacy legislation that covers the private sector, and what companies can do with the personal information that they collect and use about citizens, and how they can share that information. As of January 1st, to what extent do you think that laws that govern the private sector will be effective at protecting your privacy?

Jay: No. It's too hard. It's not that you can control where information is. There's too many ways to collect information, to share information. There's always a back door.

Moderator: There's always a back door?

Nicolai: And on that level I believe there's too much personal interest, so any time they can try to avoid those, it's not like on that level in society in politics, it's different.

Moderator: Okay. I mean, these are laws in place that say, companies can do this, and companies can't do that.

Corey: Are the companies even aware of these laws? That's another question you should ask.

Moderator: Okay. So first point: are the companies aware. Are they aware that they're following the law. Assuming that they are.

Jay: I think that they can share information or do things against privacy following the law. They always are. Like if you could have a legal message on the bottom saying "I'm sending you this email because you gave me your email." I don't know if you are really, is your income between, I don't know, \$150,000 a year, I don't know, I guess it is, so I just send it to you. But that information came from somewhere.

Moderator: Okay. Ellen?

Ellen: I think everything is never when does the company know, and how will it, are we as a public educated to know that these things are there, that we can hold people accountable for it. And, for instance, the privacy laws, a lot of cover stories a lot of stuff in the press at the time said, we don't know this is happening, and then all of a sudden you start getting information back from people with privacy disclosure statements, and can we use this, and whatever. Not very much education in relation to what it is, it can do for you, and how you can use that to protect yourself against invasion from stuff.

Moderator: Okay. Who else? Are they effective? Audrey. Why?

Audrey: My first thought is it depends on the penalty.

Moderator: Okay.

Paul: Are the penalties in place already for companies going against it?

Moderator: Well, let me answer you this way, what would need to be in place to convince you that these laws are effective?

Jay: What type of penalty?

Moderator: No, what would need to be in place to convince you that these laws are effective? Because nobody in the room is saying, a fair number of you said like you didn't believe that the governments are going to follow their own privacy laws, nobody is sort of saying that companies will follow the new privacy laws that exist. What would it need, take to convince you that these laws will be effective?

Ellen: Companies have to actually be taken to account. Either a court, or there has to be some sort of disclosure and somebody brought up or some, whatever reason, to sort of say this is what happened and these are the consequences of it.

Moderator: Okay. So, tangible proof of something happening to...

Ellen: Yeah.

Moderator: Okay, what else? If I had to leave this room and sort of take back this piece of advice, what would it be? What's going to make you believe that these laws are effective?

Ellen: Well, I think that public awareness is something. If we don't know as the public the privacy we're entitled to with corporations, then they are not on guard as much.

Moderator: Okay, so making both sides aware. Corey?

Corey: I think people should know what their rights are. Awareness, I guess. Employees and employers.

Moderator: June.

June: I don't really have anything to add, I just agree so far with this.

Moderator: Okay. Is there sort of, going to another, in governments in the past while have actually started to do a number of things on the security front, post September 11th, a number of things to increase security. At times you hear the other side, well, these measures are being put in place at the expense of privacy. What are your comments? I mean, a lot has gone on in the past couple of years. What do you think the trade-off – security, privacy?

Corey: It depends on what you value more, I guess. That's the discussion. Do you value privacy or do you value security? That's the trade off right there.

Moderator: Okay, can you think of any things that may have compromised some privacy?

Ellen: Just expand on that again.

Moderator: Well, some of the things, I mean, you earlier mentioned in terms of crossing the border and being trapped, that's an example of security measures where there's a privacy dimension. Now they track who is leaving, who's going into the country. Is that kind of thing justified? You said you didn't like that.

Ellen: No.

Moderator: Is it justified, though?

Ellen: Back to the question again. My sense is I don't think it matters sort of what security is being put in place, like if we're doing that. I think if anybody really wants to do something, they're going to find a way to do it. And if they find what security measures are in place, they'll find a way of circumventing it. So, I think you need medium security, medium security, I guess I don't know how much of my privacy wants to be constrained, I guess, I don't know how to put it.

Moderator: Audrey?

Audrey: I've lived in Israel. So you talk about privacy and security, that's a place where your purse is searched when you go into a grocery store. And it was all done in the name of – you just take it for granted. But that's an extreme example compared to the way we live here in Canada, where we're not aware of things around us that could be potential dangers, or people, we're not suspicious of people. We're very trusting. And it's just our mindset, compared to the mindset of, that was extreme, Europe is a little less so, but it's gotten where people are more –

Moderator: Let me take that example, where we're trusting, we don't haven't really done anything, and at the other extreme Israel where you walk in we're going to look at your handbag. Where on that sort of spectrum should a country like Canada be?

Audrey: It's a tough one. It's sort of new for us in some respects, isn't it? Like by-product for us. I mean, after 9/11 it kind of brought it to our continent, security issues and things like that, so we have to work with a very large country that lives next door to us. So I guess their, in some respects, we maybe have to give a little in terms of cooperation. It's really like an individual giving up a little of their privacy or something like that for the benefit of the whole kind of thing.

Moderator: Okay. Ellen?

Ellen: I think one of the scariest things that I've seen in my life is being at an airport and seeing people with machine guns. You know, and that sort of really brings the whole security issue right to the forefront. It's, I think it's a fine line, I think in some ways I'd rather have overt rather than covert sort of surveillance because then I may or may not know that it's actually there, and I actually lived somewhere once where when you got up in the morning you checked underneath for car bombs, you know? And that just became a part of your life, but that doesn't mean that I want to live like that. And I don't know that ... I think 9/11 just brought everything up into the fore, and it brought something to our continent that we hadn't had to deal with before. I don't like the idea of all the extra security around, and I don't really know how effective it is.

Moderator: So coming back to our original question in terms of you didn't like the fact that they now know that you get on an airplane and move across...

Ellen: No. I mean, I haven nothing to hide, but ...

Moderator: But is it justified? And we sort of come back to – here you're completely trapped and you don't do anything, here we look at everybody's purse.

Ellen: I think to what it boils back down to again is there have been so many breaches of security, you know all this security and what is it doing, or apprehending, or whether they're getting the right person these days, then I have less faith in, sort of the actions that they're taking, so that's my feeling on it.

Moderator: Okay. Let me see a show of hands. How many of you have participated in a customer loyalty program? Something like Air Miles, Zellers Reward, a show of hands. Any? No? So everybody but Jay. What's the purpose of these programs?

June: To get something for free, or the perception of getting something for free.

Moderator: You get something for free.

Paul: Well, with your purchasing power, you purchase, like with a Canadian Tire card you get a certain amount of points you get a certain amount of Canadian Tire money on your card, which you can transfer into actual goods from the catalogue and stuff like that.

Moderator: Okay.

Jay: They are to make you buy more, like sort of an incentive? Also, I think it's tracking your movements, what you buy, and how.

Corey: For marketers, the purpose is to collect the database so they can do more targeted marketing programs. Like Optimum cards are the biggest marketing program at Direct Marketing Canada, in North America.

Moderator: Okay, so to try to sell you more, to keep track of what you buy, which they use to what end?

Ellen: But can't they do that anyway, I mean, they can keep track of how you spend your money.

Jay: They can with your debit card, but with cash, they can't.

Corey: When you use the Optimum, they know what you bought, what products you bought and everything, it's the most specific database possible.

Moderator: And what do they do with that information?

Corey: You get offers based on your buying patterns I guess.

Moderator: Okay. Kind of spam you with...

Corey: Targeted marketing.

Ellen: As opposed to untargeted?

Jay: Some of the companies that make the product, they are interested in that information to know what the people want, what person liked this product that we made two months ago.

Nicolai: But that's good.

Moderator: That's good? Why?

Nicolai: Why? Because they will receive the signals of what the society needs, if they don't need something, there is no need to spend money to produce it. I believe that. They cannot make you buy more, you can buy whatever you want to possess. You cannot buy more. People go into straps with the credit cards, but you have to think, you cannot make mistakes. The decision is yours, by the way.

Moderator: Jay, why don't you, you're the only one in the room that doesn't. Why not?

Jay: Because my wife has it.

[Laughter]

Moderator: Okay. Why do all the rest of you participate in these kind of things? Why do you have an Air Miles card? Why do you have a Club Z?

Corey: To get rewarded for your regular shopping.

Nicolai: To get some more value for something, because you have to buy anyway, right? So if you're going to get something else ...

Ellen: In some cases, there are only so many places to buy things, like for instance the drug store market is a little bit narrower, there's Shoppers Drug Mart, there's PharmaPlus, and then there's some

independents, so it's like putting your eggs in one basket, you hope that you get more points. Plus it helps them to keep you as a customer.

Moderator: Okay. What do they do with the information that they have on you? Can they sell it to other companies?

Ellen: Yes, I think so.

Moderator: Well, basically you're right, I mean, that's what the Air Miles will do, each time you use the card you collect points. They keep track of the items that you've purchased, and then, in essence they can sell the purchasing behaviour to other companies participating in the Air Miles loyalty program. So that doesn't bother you, in terms of being able to track everything that you buy? Any issues there? June?

June: Not really, no. It doesn't really bother me.

Moderator: And what do you think about them translating the information to other companies.

Ellen: It's the fine print on the agreement we sign, I think.

June: Sometimes they give us a choice and we share it, sometimes it's right up front there, it's nice to see that because then you are prompted to say yes or no kind of thing, which is good.

Moderator: So presumably, you sign up for this, they ask you about all your purchases, but also how old you are, your household income, your gender. Is it okay to share that kind of information? So now they have your buying habits, they have who you are, and you have a nice neighbourhood.

Jay: I don't really see the [?] of having that information. I see the government, if they are tracking so I don't feel more secure, but in this case, market information that I don't really think – I would like to have my own, I would like to choose the stuff they offer me. I don't know, it's a different viewpoint.

Moderator: Anybody, any issues there? This is all fine, doesn't matter?

Audrey: It doesn't matter to me because I know I'm doing it, and I know that that's the cost of admission, so to speak.

Moderator: Ellen?

Ellen: I do it because I want the advantages of it. And I have one card and I use it.

Moderator: Well, I've heard a little bit about the issue of monitoring earlier. So let's turn to the issue of surveillance cameras. How are surveillance cameras being used today, where you live?

Ellen: For security purposes, for one thing.

Moderator: Okay, security purposes. So in your grocery store, local convenience store.

FP: Where you live, if you live in a high rise apartment building, there's probably security cameras there.

June: It's at the office too.

Moderator: Surveillance cameras? How?

June: Well, first of all they could be downstairs in a common area of the building, but a firm can also elect to have them installed in their corridors and doorways and things like that. It's well known that people are able to break through security and are sort of coming right in behind you if you're not alert to that sort of thing. There's theft that goes on, people carting out all kinds of equipment and things like that.

Moderator: How else are they being used?

Corey: In casinos, they use them. They have a database of profiles they have and if someone matches that database, they can take an image of their face and red flag it, I guess for security purposes too they can do that for airports.

Audrey: I know they're used for research.

Moderator: They're used for research? In what way?

Audrey: Marketing research, shopping patterns, and also in office planning we use them for how we use offices. And that's all done, they sign waivers.

Moderator: So in an office, let's use that as an example, do they know that they're being ...

Audrey: Yes, they know that they're test subjects for the research.

Moderator: What about how are they being used elsewhere in the country?

FP: Traffic, photo radar, the tolls.

Ellen: Some countries actually have them set up in the main streets, at sort of strategic points so that they can sort of check patterns and people.

Moderator: In London, England, and in fact in some Canadian communities – Kelowna, BC is sort of the most known example, police are actually using surveillance cameras to monitor public places in order to, they say, deter crime, assist in prosecution of offenders, and I think in London, in fact, there are approximately 150,000 surveillance cameras all across the city monitoring public place. When I tell you there are 150,000 across the city of London, what do you think of that?

June: Well, they have, of course, have problems with that little island across the way from them, in terms of terrorism acts and things like that, so maybe that's one of the reason they have a heightened concentration of cameras and surveillance.

Moderator: What are the pros? I mean, there are obviously pros and cons to anything like this. What are the pros?

Jay: Security.

Paul: Yeah.

Corey: It would be interesting to compare the crime rate of their city versus another city that doesn't.

Jay: Or the time before the cameras.

Moderator: What other pros?

FP: Safety.

Moderator: Safety.

FP: Prevention.

Moderator: What about the cons?

Paul: Invasion of privacy.

Ellen: Also, in a democracy it's the right to assemble, I mean, so if the police are watching people assembling they're going to prevent it – wait a minute ...

Moderator: Okay, and there's both sides. Some say that they are effective at reducing crime, others say they're not effective. If you had to state your own opinion, do you think the 150,000 cameras in the city of London would be effective at deterring crime? Yes or no.

[Responses:] Yes. No. No. Yes. Yes. No. Yes. Yes.

Moderator: A bit of a division. Why no?

FP: Well, it depends, I mean, sometimes you may be aware of the cameras and other times you may not. If you're aware of them, you can always relocate to somewhere where there's no camera. Don't do it right under the nose of the camera.

Ellen: If you knew that there's cameras around, if somebody was going to be attempting something, they may either do something in the way of disguise or they would try to identify where the cameras were and go around them.

FP: Or disable them.

Moderator: The other thing, though, Corey said no, right?

Corey: I said yes.

Moderator: Audrey said no. Why?

Audrey: I just agree with them.

Moderator: What would you think if a city like Toronto was to follow the lead of London and introduce 150 or 200 thousand cameras across the city? Basically in London they cover with 150,000 it's a relatively small city, it encompasses the city. What would you think of the idea of doing something similar in Toronto?

Corey: I think it's under the assumption that crime only happens in public places.

Moderator: What do you think of the idea?

June: Besides the fact that we couldn't afford it?

Moderator: Putting that aside.

Jay: In other cities the crime rate is so low I would look where are the crimes.

Moderator: So you don't see a strong risk that the invasion or privacy outweighs the perception of the risk in the city.

Corey: I don't think there's a need for it.

Moderator: Why?

Corey: Crime isn't that bad in Toronto. There's other cities that could use it, I mean, I think that people want to invest the money into those cameras, there's other high priorities that people want invested

money into. It wouldn't fly, that idea, I don't think. If you were putting it in health care, or education, maybe.

Moderator: Okay.

Nicolai: I believe it's effective because instead of police cars chasing criminals and making the situation worse, those cameras can pinpoint the direction, it would be easy to stop them or these shooters who kill teenagers or people around the bars, they will be caught on this camera and they will not be searchable because they will know who they are. The pictures are there. Now, they don't catch them, they don't know who they are this way.

Moderator: So good idea, what do you think of the idea in Toronto?

Ellen: I wouldn't have thought it was necessary. I think that I agree with what everybody just said. Plus I think that technology is always changing, so if this is an investment that you would be making on a regular basis, and would the money be better spent putting it in, if there was crime, in the bits and pieces that lead to it. You know, whether it's homelessness or poverty, or education or whatever, of putting it where you're going to prevent it at this point.

Moderator: Anybody else? Corey. Good idea or bad idea?

Corey: I think it's a bad idea.

Moderator: Just from a cost perspective?

Corey: I think that you've got to show proof to the public too that there's a need for it, that it's effective. That it works, this is a huge investment, I'm assuming, but with all this money, you don't know that it's going to do what it's supposed to be doing.

Moderator: How many are comfortable with the idea? Because I know, for example, that this there's one in Kelowna, BC in the main part of downtown. How comfortable are you with the idea of being monitored by a police surveillance camera as you walk around a street or park?

FP: It doesn't sound very nice, the idea, it doesn't sound too appealing.

Moderator: Doesn't sound appealing, are you comfortable with it?

Paul: But you wouldn't be individually monitored. It would just be certain sections of the area you're into, right?

Moderator: But they could keep track of individuals going through that area. Would you be comfortable with the idea? I mean, I've heard a cost issue, that's a fair point when resources are scarce and there's not enough for health care, but aside from the cost issues, are you comfortable with the idea.

FP: No.

MP: No.

Jay: In places where there's a huge amount of people, in places like that, like what happened in Madrid with the rail car, it can happen here. And this point is, I think I would feel bad if we put a camera in and we had a relaxing time with people.

Antonia: No. I wouldn't mind if it was in certain areas, and I know where they are.

Nicolai: For example, there are cameras elsewhere in the subway, nobody mentioned that that bothers them. So, would it be the same in the other places, and I don't believe cameras are so expensive today.

It's not something very very expensive, it's like major electronics now, you can go and purchase for \$50 VCRs, it was \$200 ten years ago.

Corey: But it's not just the cameras, it's the cost of maintaining it too. The labour behind it, people who are monitoring the cameras, that's a lot of different people.

Paul: You said there are surveillance cameras already in the subway station. What is that, like three or four in each station?

Nicolai: Each subway has cameras.

Moderator: What just happened in Spain and the bombings there, and you said like the park that goes through my neighbourhood versus a place where there are a lot of people going, you have to go down University, or Bay Street during a weekday and how many people are out there. What about the idea of having cameras in certain parts of downtown Toronto?

Audrey: There already are.

Ellen: A lot of those buildings have cameras on the outsides of their buildings, the entrances and things.

Moderator: Those are more individual, that kind of belongs to the building. Some of the ones in London belong to the police.

June: That wouldn't make me feel any more secure.

Moderator: Okay, I'm going to hand out something. I'll get to you read. So basically you're all people in the area of privacy. They talk about four different types of privacy: bodily privacy, communication privacy, informational privacy, and territorial privacy. And in the handout there are sort of examples of what they mean by that. So the first question, I want you to rank the different types of privacy in terms of how important it is to ensure that your privacy is maintained in these four areas. So I want you to put a one, two, three, or four in terms of which type where one is the most important, and four is the least important. And then I want you to rank the same four in terms of the degree to which these areas of privacy are under threat for you personally. So one could be the one that is most under threat today, and four is the least under threat today.

[Pause]

Okay, four different types of privacy with fancy labels that are referring to different things. How would you rank them? Paul.

Paul: For the first part I put communication one, information two, bodily privacy three, and territorial privacy four.

Moderator: Okay. Ellen.

Ellen: Two, two, one, one.

Moderator: Two, two, one, one. Okay. You cheated, right, you didn't assign all the numbers. You were supposed to use one through four. One is the most important to you and four is the least important. So those who didn't do a one, two, three, four, just go back and say, well, this one's more important than this one. And the second part of the question the same thing. Okay, Nicolai, how did you answer? What was your number one?

Nicolai: The first part: four, two, three, one.

Moderator: Okay, can you read them in the order...

Nicolai: You mean which one? Territorial privacy is one, two is communication privacy, three is informational privacy, and one is bodily privacy.

Moderator: Antonia.

Antonia: Bodily is one, communication two, information three, and territorial four.

Moderator: Audrey.

Audrey: Communication one, bodily two, territorial three, informational four.

Moderator: Corey.

Corey: Territorial one, communication two, bodily three, informational four.

Moderator: Jay.

Jay: Territorial one, information privacy two, communication three, and bodily four.

Moderator: June?

June: Communication one, information two, bodily three, territorial four.

Moderator: Ellen?

Ellen: This is for the second half?

Moderator: No, the first one.

Ellen: Bodily three, communication four, informational two, territorial one.

Moderator: Okay, that's sort of equal. What about the second question? And then read them in the order of one, two, three, four.

Paul: Information one, bodily two, territorial three, communication four.

Moderator: Nicolai.

Nicolai: I used the same, because I assume hypothetically that this the way I don't want to be changed in this way. If I put one as territorial I meant that I don't want, let's say, to be disturbed at home. I mean, if I don't want, that's why I use it. Maybe I made a mistake. Is that different from the understanding I took of the statement. So I did one territorial, two communication, informational three, and four bodily.

Moderator: Okay, Antonia.

Antonia: Informational one, communication two, bodily three, and territorial four.

Moderator: Audrey.

Audrey: Informational one, communication two, territorial three, bodily four.

Moderator: Corey?

Corey: Informational one, bodily two, communication three, territorial four.

Moderator: Jay?

Jay: Informational one, communication two, bodily three, territorial four.

Moderator: June?

June: Information one, territory two, communication three, bodily four. Exactly the same.

Moderator: Okay, we've been talking for almost two hours on the issue of privacy. What do you think is different, if you're going to leave this room obviously it's not the kind of issue that you talk about in this kind of detail on a daily basis. What is different in your mind than what was when you first came in this room not knowing what we were going to talk about? Jay.

Jay: What Ellen said about the laws. Now I know that they're in place and I will feel more comfortable, more confident that the information is keeping place, even though she herself doesn't believe it.

[Laughter]

Moderator: Okay, June?

June: I think just maybe the onus is a bit on the individual to become more aware of what maybe the privacy laws are, just for information purposes so we can conduct ourselves accordingly.

Moderator: Ellen?

Ellen: Just maybe realize that you really need to talk about these things and then you need, what I want to do is go and sort of act and do some stuff in relation to it so I don't get more junk mail, and put some more pieces in place. Protect my privacy a bit more, you tend to let it slip.

Moderator: Paul.

Paul: Just that companies and things, and governments do have access to all sorts of things about you, but you yourself have the wherewithal and the different controls to protect what privacy is leaked to other people.

Moderator: Okay.

Nicolai: In general, first the satisfaction that because at least somebody, someone would like to hear my opinion as a private society and ordinary person. Optimism that somebody will get the message from the public, it's a society, different presentation, in order to do, as we said, because in some countries there is no one to ask you, they decide, and that's it. You are like a sheep, like cattle.

Antonia: Sorry, can you repeat what you said?

Moderator: So I mean, we have been talking about privacy, I mean you've just come into the room, you've been talking for almost two hours about the privacy, obviously not something that a lot of people talk about in this kind of detail on a day to day basis. What's different now that you're leaving the room having talked about this?

Antonia: Well, for me, now I know there's actually laws out there to protect your privacy. I didn't know that before.

Moderator: Audrey?

Audrey: I wasn't aware of the new laws, so now I have to go find out what they are.

Moderator: Okay. Anybody more concerned? Less concerned? About your privacy in general.

Corey: Same.

Antonia: Less.

Moderator: Less concerned.

Paul: Same.

Moderator: Ellen?

Ellen: Same.

Moderator: Same. If you want to find out more, you can put, go to the Office of the Privacy Commissioner of Canada, so if you went to the Government of Canada's main website, which is www.gc.ca and then their under the Privacy Commissioner of Canada, there's a lot of background information on privacy legislation. It is almost 7:25, and I promised to have you out on time. Thank you very much for taking your time out of a busy evening, and I would ask you to sign out on your way in. I'll get you just to rip off the paper. Thanks a lot. Have yourselves a great night.