HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 045 • 1st SESSION • 41st PARLIAMENT

EVIDENCE

Tuesday, June 12, 2012

Chair

Mr. Pierre-Luc Dusseault

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, June 12, 2012

● (1205)

[*Translation*]

The Chair (Mr. Pierre-Luc Dusseault (Sherbrooke, NDP)): As we have already lost an hour to voting, we will move without further ado to witness presentations, for 10 minutes each. We will then have a question and answer period. We also have committee business on the agenda. We may have to continue the meeting after 1 p.m., if we agree. We will begin with the 10-minute presentations.

Mr. Kerr, go ahead.

[*English*]

Professor Ian Kerr (Canada Research Chair in Ethics, Law and Technology, University of Ottawa): Good afternoon.

Almost exactly one year ago I was sitting in a boardroom much like this one, only much, much fancier. The daylong meeting was at 1601 South California Avenue in Palo Alto, California. If the address isn't familiar to you, it's the Facebook campus. A guy called Mark Zuckerberg works there. It is spectacular—vibrant, pounding with energy, everybody jacked into headphones. I felt like a kid in a candy store.

Because I was required to sign a non-disclosure agreement upon my arrival, I cannot tell you many of the interesting things that I learned at Facebook that day. Apparently Zuck's Facebook tag line, which reads—and I quote—"I'm trying to make the world a more open place by helping people connect and share", does not apply to Facebook's business operations.

However, there is one thing that I will disclose: I got sick to my stomach that day from eating way too many Sour Patch Kids. The roof of my mouth was practically torn to shreds. Imagine a very well-stocked candy store—Sugar Mountain or the Bulk Barn—with a seemingly endless supply at every single coffee station throughout the entire Facebook campus.

Now, in defence of my gluttony, let me say that I was not the only one. What I witnessed that day was 25 of the world's most important privacy scholars and advocates stuffing their faces, lining their pockets, and filling their knapsacks with candy—grown adults earning six-figure salaries. We weren't stealing. Excessive and free consumption was encouraged. We were simply reacting to the offer of ubiquitous, abundant, and highly addictive forms of fuel.

Why have I wasted three of my precious ten minutes talking to the ethics committee about eating Sour Patch Kids at Facebook's campus? Because information is the new sugar: big data, big sugar—get candy, get candy, get candy.

Just as health practitioners urge us to consume fewer refined sugars and to safeguard through policies the increasing unhealthy consumption habits of Canadians, I appear before you today as a privacy practitioner, urging you to safeguard Canadian citizens and global corporations from the complex and increasingly unmanageable desire to collect, use, and disclose more and more personal information.

Because big data is like big sugar: the more ubiquitous, abundant, pleasurable, efficient, and profitable it is, the more we want it. Sometimes, the more we want it, the more blinded we are by its consequences. We stand at the precipice of what one might call the late onset diabetes of the information age, and we should be doing much more to prevent it.

You've already heard excellent submissions from two fantastic commissioners, Ann Cavoukian and Elizabeth Denham, as well as my hugely talented University of Ottawa colleagues, Professors Scassa, Geist, and Steeves. They have overlapped on a number of crucial recommendations that must be followed by this committee. I'll recap four points quickly.

First, you need to finish what you started. You're way behind on a number of necessary legislative reforms to PIPEDA, the Personal Information Protection and Electronic Documents Act. Studying social media may grab headlines, but the ethics committee should first focus on the PIPEDA review. I learned as a kid to leave the drum solos to later. It's not as sexy, but the rudiments must come first.

Point two: perhaps the most important rudimentary aspect of this is that the Privacy Commissioner needs much greater powers, including the power to make orders, award damages, and issue penalties. These enforcement powers must have serious teeth.

Point three of the overlap—also rudimentary—is mandatory notification requirements for a certain kind of security breach.

The fourth and last of the basic points I'm reiterating from the previous discussions is the need to mandate far greater transparency, not only about the collection of personal information, but about how it is being used and to whom it's being disclosed. We need this both at the front and at the back end of social media transactions.

To be clear, this is not just a point about tweaking privacy policies or making more understandable notice provisions. It is about legislating what I would call mandatory minimums—mandatory minimum standards for privacy transparency, requiring that they be embedded into technologies and in social techniques. We don't sell cars without speedometers, odometers, or fuel or pressure gauges. Likewise, our social media should be required to have feedback mechanisms that allow us to look under the hood and to warn us when conditions are no longer safe.

● (1210)

I have two further submissions of my own. The first concerns privacy of default settings. In his appearance before this committee, Professor Geist generously referred to my work entitled “The Devil is in the Defaults”. In short, the architecture of every technology includes a number of design choices. Some of those design choices create default positions. For example, a car's default position is stop. When we enter a car and turn it on, the car is in park. For safety's sake, its design requires that we conscientiously put it into gear in order to go. Although it would be possible to design things the other way around, we recognize the danger of cars that default to “go” rather than “stop”, and we have regulated against them.

The same should be true for privacy, but it isn't. For example, following the lengthy investigation of Facebook in 2008 and 2009, the Privacy Commissioner found that Facebook needed more privacy safeguards. Responding with a complete overhaul of its so-called privacy architecture, Facebook offered new settings for its nearly 500 million users. Although this was deemed a privacy U-turn by the major media at the time, the net effect of these new settings was ironically a massive and unprecedented information grab by Facebook, which I would be happy to explain more in the question period.

In a rather subtle and ingenious move, Facebook very politely gave our Privacy Commissioner the new settings she wanted. But when Facebook gaveth, it also swiftly tooketh away. Choosing to create privacy default settings that collect more information than even before, Facebook knew perfectly well that 80% to 92% of its users would never change those defaults. Behavioural economics made it very clear that, like a bad sugar habit, Facebook could get away with nudging us further and further towards poor information consumption habits.

Currently, the Privacy Commissioner is powerless to do anything about this. Without changes to our law, Canadian legislators are allowing social media sites to build vehicles that default to “go” rather than “stop”. Zuckerberg knows how unsafe this is. This is why he has rejigged his own privacy settings. He knows that Facebook's defaults are dangerous. The question is why isn't what is good enough for the geese also good for the gangster?

The devil is in the defaults. We need to fix this through legislation that contemplates settings with privacy as the default. While I agree with Professor Geist that Twitter should be commended for “Do Not Track”, and that Google should be commended for its privacy dashboard, I would take this all one step further. We need legislation that would make some of these amazing features on our online experience non-optional. They should be factory-built and installed with privacy as their default.

I will make my second submission much more succinctly, since it's similar to the testimony I offered at the PIPEDA review a few years ago. The biggest threat to privacy is not social networks. It's not surveillance cameras. It's not wireless mobile, nor databases, nor GPS tracking devices, etc., etc. The biggest threat to privacy is the standard form contract. Under our current law, almost all privacy safeguards that are built into our privacy legislation can easily be circumvented by anyone who provides goods or services by way of a standard form agreement. By requiring users to click “I agree” to their terms on a “take it or leave it” basis, companies can use contract law to sidestep privacy obligations. In short, this is based on a mistaken approach to the issue of consent. In my written submission, which I will provide to this committee, I offer detailed legislative reforms that would help prevent companies from doing an end run around the protections set out in privacy legislation. It's crucially important.

Thank you for your consideration of these matters. I hope during the question period that committee members will give me the opportunity to expand on my three main recommendations: one, mandatory minimums for privacy transparency; two, mandatory privacy default settings; and three, mechanisms that prevent contracting out of privacy through standard form agreements.

Thank you.

● (1215)

[*Translation*]

The Chair: Thank you for making your presentation.

I now yield the floor to Mr. Levin for 10 minutes.

[*English*]

Professor Avner Levin (Associate Professor and Director, Privacy and Cyber Crime Institute, Ryerson University): Thank you, Mr. Chair.

Thank you very much for the invitation.

The clerk was kind enough to circulate a brief, but in the interest of time I will just leave it with you and take that brief as more of a departure point.

I would say that main point that our written submission presents is disturbing. People say that they care about privacy, but they are not really prepared to take individual action when you make the tools available to them. To that extent, some companies have taken positive steps by allowing users, whether it's Facebook or Google, to see what's available to them individually, but we see the same kind of disturbing pattern.

At the same time, the disturbing pattern is, I believe, a call to regulatory action. I don't see any reason why I should discount people's deep interest and respect for the rights of privacy and favour that less than perhaps their desire to take or not take action.

So we have valid concerns around privacy and we have individual action that is not at the same level. What does that all require? In my opinion, it requires some kind of action.

Now, when I thought about that proposed course of action would be, my thoughts were these. You've heard very eloquently from Professor Kerr and others about how PIPEDA should be reformed, about the amendments and how they have so far failed to be on schedule, etc. In my opinion, the regular amendments won't actually help that much when it comes to privacy in social media.

I think it's because—if you'll allow me a short segue—we have larger problems regarding social media and privacy than the ones that just come through with the online advertising and the monetizing of personal information, which is a significant problem, no doubt. There is a notion that is very relevant to social privacy, and it's the notion of network or contextual privacy, which I want to talk very briefly about.

This makes us aware of another puzzle. We all know that people say they care about privacy, yet they post a lot of information about themselves on social media. It's always difficult for people to square that. How is that possible? Why don't people realize what they're doing? Don't they understand that it's public, etc.?

The key to understanding that is to understand that people, when they share information or they post information, don't actually think about how many people potentially have access to the information; they are really focused on who has access to that information at that point in time.

That is the way that people actually behave in the real world. That is not unique to online. That is how we behave in our daily lives.

I'm here to you presenting in my role as an academic, but I also have other aspects to my life that you may or may not be aware of. For some of it, you can perhaps Google me. If I were on Facebook, you could probably get a lot of information about me there. But in regular life, you may not know, for example, that I have two daughters. You many not know anything about my family status, and you may not know, for example, about my religion, that I'm Jewish.

We in our regular life have the ability to keep our identity and our information directed at particular audiences as we see fit. What happens with social media is that it takes away that power from us to do that.

That is the basic issue we need to confront. We have real boundaries in the real world, and the boundaries are being blurred in the online environment. It harms our privacy, and more fundamentally it harms I guess our sense of identity, especially with young individuals and how that identity is developed, their potential career paths, and many other issues that relate to the ability to keep information segregated.

I want to point out to members of the committee, although perhaps you're aware already, that under the Privacy Commissioner's interpretation of PIPEDA, all of this problem is not commercial information-related, and therefore not to be addressed under PIPEDA. When the Privacy Commissioner did her Facebook findings in 2009, this kind of use of information that crosses perhaps from one user to another was not deemed to be commercial.

● (1220)

There's a question you have to ask yourself, then, when you think about Facebook and other social media; that is, what is it? Is it a social network for people to socialize on, or is it a database in which information is collected? I would say that in this day and age it's probably both, and what the committee needs to remember is that you cannot focus on one and forget the other. You need to worry about both of them.

How do you do that? I would say that you probably have to do some fairly radical changes to the privacy legislation model that we have now and that has been in existence for 30 years in other countries and, in one form or another, since the mid-nineties in Canada.

I would say that it probably would be a mistake to sort of.... Or perhaps we have to accept as inevitable that the collection of personal information and the disclosure of personal information are pretty much a fact of life and are here to stay in the current social media environment. What we need to focus on, I suggest, is how that information is used, what forms of use are permissible, and what forms of use should not be permissible.

The analogy I would present to you would be the analogy of the prohibited grounds for discrimination you are familiar with from the charter and right down to the provincial and Canadian human rights codes. If you remember, there's information there that is readily available to people when they want to make an employment or housing decision—for example, information such as a person's colour, age, sex, and disability or not—but we have laws that do not permit action on such information. We have to come to grips with the notion that online information may be available and how we then are going to allow or not allow the information to be used.

I would say, of course, that not all the information that originates online or in social media should be prohibited. I can give you, for example, a suggestion that if the information indicates some kind of criminal conduct, perhaps we would want that use to be permitted. But I would suggest to you that if the information that is coming online has to do with somebody's private life, for example, such as their religion, their family, their disability, or anything else, we should not allow people to use that information. When I say “people”, I mean that advertisers should not be allowed to use that information, potential employers should not be allowed to use that information, app developers should not be allowed to use that information, and so on and so forth.

My suggestion to the committee is to really consider—because of the situation Canada is in, where there hasn't been a major substantive amendment to PIPEDA over the last few years—that the problems social media present are much more serious, I will say, for privacy and people's sense of identity than just the focus on the collection of information. We really have to think and be forward-looking in order to create some legislation that would withstand the test of time, for at least the beginning of the 21st century, let's say, and to focus on what permissible use of that information would look like and what are the rules and constraints that we want to do around that. That would be a suggestion I would make to the committee, and I would welcome any questions or further discussion on it, if we have time for questions.

Thank you very much.

● (1225)

[*Translation*]

The Chair: Thank you.

I now yield the floor to Mr. Gautrais for 10 minutes.

Dr. Vincent Gautrais (Full Professor, Université de Montréal): Thank you, Mr. Chair.

I would like to use my 10 minutes to share the opinion of someone who is not quite an expert on privacy issues. For some 20 years now, I have been interested in the relationship between the law and technology. It is from that perspective that I would like to expand on three points. Very often, I discuss those points to deal with the complexity that characterizes new technology. Those three points are very simple: who, what and how.

Let's begin with the "who". Who should take action when it comes to those issues? I would like to begin with the first instinct we have—that of thinking that the legislator should act in such matters. I would nevertheless like to repeat the opinion of an old civil lawyer who said that legislating should be done carefully. This means that, in such a new field—which is so poorly controlled—adopting a piece of legislation very quickly is often a factor that prevents our habits from developing.

Therefore, I think that, in terms of legislation, we should be careful. We should take a step back and focus more on establishing a strictly minimalist approach in legislation, without developing, in my opinion, any new concepts. We have seen such concepts in Europe—including the "right to forget", which was developed in a number of European pieces of legislation and seems to me overly difficult to apply.

Conversely, even if the goal is to limit the legislator's role, it does not mean that nothing should be done. There are some possibilities when it comes to privacy management as far as organization goes. I think that the options established in Bill C-12 are very interesting, especially with regard to providing the Office of the Privacy Commissioner of Canada with a bit more power.

This means that my second stakeholder in terms of privacy is the Office of the Privacy Commissioner. Let's compare what we do here with what is done elsewhere, in all of western democracies or, at least, in Europe. If we compare ourselves with countries such as Germany, Sweden or France, we realize that the office has fairly limited prerogative powers. Overall, the resources and the number of people who work within the Office of the Privacy Commissioner are, in Canada, half of those in Europe. I feel there could be some more resources to help develop habits. That's something I will talk to you about later. So it's a matter of informal standards in terms of privacy management.

As for the third stakeholder that would be likely to act in privacy matters, I have in mind organizations themselves—in other words, companies and public organizations that manage data. Pursuant to a point I will develop later on, I feel that those organizations are becoming increasingly accountable when it comes to the way they must manage personal information. The notion of accountability is hard to render in French. It has developed in all international fora—increasingly so over the past few years, or since 2004-2005. The notion of accountability is a concept that, in my opinion, should be promoted in this committee's projects.

So there you have the "who", and that's what I had to say about the stakeholders who should be involved in those issues.

Let's now talk about the "what". I would like to use a single sentence to summarize my thoughts on this: I fear the shade much more than the light. What do I mean by that? There are many fantasies and fears when it comes to social media. There are of course some genuine fears. My opinions differ from those of my colleagues, but there are some real fears. There are also some imaginary fears. In some respects, what I can put on a Facebook page does not frighten me at all. I encourage my three children to use Facebook, but I am sorry to say that they don't want to.

However, it's quite possible to use Facebook without privacy being affected. If schools and the Office of the Privacy Commissioner educate us, we should be able to manage that. I am referring to Twitter. Two days ago, the office posted a cartoon on Twitter to explain how people should manage privacy. That kind of a solution is not of a strictly legal nature. Law is not the only possibility in life; there are other solutions that can help change Facebook or Google users' behaviour.

● (1230)

In many ways, I have no fear of how Facebook may use information. I am also not worried about Google Street View, and that is something I would like to discuss. I am bringing this up because the Office of the Privacy Commissioner has made some recommendations against Google Street View. However, Google Street View is not dangerous. I have no problem with being seen in front of my home taking out the garbage. This is one example of imagined fears that are sometimes associated with social media.

That being said, there are nevertheless real problems and fears. We must keep an eye on new behaviours, and I agree with my colleagues when it comes to that. What scares me more is when the objective is changed, the reason why information was placed on Facebook or Google. In many respects, those changes of objective are made through a contract no one reads. An average social media user would have to spend 20 hours a month to read the privacy policies that apply to Google and all the websites they visit. That is unfeasible. Saying that protection goes through information and consent is an illusion. As Professor Kerr mentioned, that is a totally inapplicable legal tool.

As my colleague was saying, there are some cases where consent should not be given. For instance, some law firms—in Quebec and the rest of Canada—ask their students for their Facebook account to see who they are in real life. Such cases go against the law, and a judge could consider them to be a violation of the law. In fact, it may be useful to explicitly state that in a piece of legislation.

I have covered the “what”, but I will now talk about the “how”. I would like to come back to the notion of accountability, which is becoming increasingly developed. According to that notion, organizations must establish policies that will make it possible to objectify, if I may put it that way, their diligence in managing personal information. Forcing Facebook, Google or any other public sector company or organization to show everyone how they manage data internally would be a way to check how diligent they are. That notion is fundamental and very useful. It is actually the basis of an agreement concluded last November between the Federal Trade Commission, in the U.S., and Facebook, whereby the latter committed to open its books and show its management of data over a 20-year period. The future lies in the notion of accountability.

Once again, we have to be careful. This is coming from a technology expert who goes beyond the notion of privacy. There have been some rather unfortunate cases, especially in the area of securities. In 2002, several financial scandals erupted in the United States. To remedy that situation, all companies listed on the stock exchange were asked to open their books and produce internal reports to show how they were managing financial information. Many U.S. authors showed that large quantities of documents had been produced and financed by accounting firms, some of which were at the source of the financial scandals. Some $60 billion or $70 billion later, they ended up with a magnificent documentation that, in the end, is sometimes difficult to apply.

That is why this notion of accountability should not be introduced through a piece of legislation, but rather through informal practice standards, through codes of conduct. With a more negotiated approach, there would be no law imposing things within a generally quite short time frame, and the situation would be conducive to dialogue for establishing practice standards. Informal standards and codes of conduct are often criticized because they are not restrictive enough. When I compare our privacy system with the European one —with fairly substantial resources for monitoring the strict application of the legislation—it seems to me that a more in-between approach, a more negotiated approach, could have better results.

● (1235)

Thank you.

The Chair: Thank you.

I will turn on Ms. Borg's microphone, for a seven-minute question and answer period.

Ms. Charmaine Borg (Terrebonne—Blainville, NDP): Thank you very much.

I would like to thank the witnesses for being here and for their very interesting presentations.

Social network users are under the impression that those services are free. However, given the progression of this study, we are becoming increasingly aware that we pay for those services with our personal information.

My question is for Dr. Kerr and Professor Levin. When we put our personal information on social network websites, where does it go?

[*English*]

Prof. Ian Kerr: Shall I begin?

Ms. Charmaine Borg: Sure.

Prof. Ian Kerr: Professor Levin probably has more expertise on this than I do, but I think the important thing....

I used the phrase, when I made my submission, about there being both a front end and a back end. In terms of answering your question on where this information goes, I would first want to connect this to something that Professor Gautrais said. He had talked about, both with Facebook and Google Street View, there being some things he's just not that worried about, not that concerned about—for example, if the street view mobile is going in his neighbourhood when he's taking out his garbage. Certainly I understand and see those as comments about the front end. The back end is where these difficulties are.

Your question is a fantastic one, and it's one that I don't think any expert you could call in Canada would be able to answer with adequate precision to satisfy it, or at least as I would want to have an answer to that question. One of the reasons for that is precisely because—as I tried to sort of hint at with my actual trip to Facebook, where the first thing I was asked to do was to sign a non-disclosure agreement—much of the value of that information.... And this does not result in free transactions with Facebook, as you are paying dearly through the costs associated with that personal information. Much of the value of that information is laden with the idea that it's information about things we don't necessarily know about.

It's really important to understand here that one of the things that make that information so valuable, and it therefore gives us a sense of what's happening with it, is that this information is being utilized to create sets of what we might call “social categories”. We're all being placed in social categories, on a daily basis, on the basis of information-processing.

I know that a number of you as members of Parliament often fly to your constituencies. Air Canada, for example, will know very well if you're an elite passenger, a prestige passenger, or just a regular, everyday passenger. You will be put into a social category that, for example, in that instance will allow you to see different flights that are available on the plane, etc.

When I fly and the woman next to me says “Oh, we're so lucky we got this row with the extra legroom”, I know that she may be lucky, but I'm not that lucky: the reason I got that row with the extra legroom is that I fly a lot. Air Canada knows that, and it rewards me with the ability to choose that flight. She got the crammed-in seat in the corner, but she got a bit of extra legroom. She thought that was a matter of luck.

The point I want to make is that the information is used to put us into social categories, and those categories affect our day-to-day lives. In some cases, it's where you get to sit in an airplane, if you get a good seat or a lousy seat. In some more serious examples, choices are being made about us that could have discriminatory effects to the extent that Professor Levin was talking about.

The point is that all of these information and social media companies and other information brokers will partner with whoever they want to in order to make lucrative arrangements, the purpose of which is to do things to connect those bits of information in order to create certain kinds of profiles about us so that they can put us into categories for certain purposes that benefit us, etc.

As to how, exactly—those details would not be something that you would be privy to, or I would be privy to, unless we were to somehow summons these people and make them speak under oath about it. I signed a non-disclosure agreement. There are some things I know that I can't actually tell you without you taking greater powers to get that.

The real point is that this is so much a mystery from our end; the part that's not a mystery is the part that we know, which is that social categories are being created. Those are the things we should be concerned about.

● (1240)

[*Translation*]

Ms. Charmaine Borg: Thank you.

Mr. Levin, did you want to say something?

[*English*]

Prof. Avner Levin: Thank you.

I think that a short and perhaps unsatisfactory answer is that what happens to the information is that it's sold, right? We know that. That is the business model of these organizations. That is why they went with the biggest IPO in history, which a lot of people are somehow taking pleasure in seeing flounder, I guess, depending on whether or not you've purchased stocks.

But it is sold. I'll give you an example from Twitter. Twitter sold I think the last two years of feeds to two marketing companies, which would then create that sort of segmentation based on products. So we have companies that are interested in mining the information. These are all kinds of tweets—personal and whatever—but they look for various products, issues, etc., and they use them to then target ads. We have to understand that as long as the service is free—on the face of it—that is how these businesses are going to justify to their investors that they will make money.

I have to say at the same time that, again, when you look at individual actions and ask people what their preference would be, in our research, only one in five Canadians would pay $1 a month to avoid the collection of personal information, and 30% would be willing to be paid $1 a month to get targeted ads. So there is a challenge here, and what I would say to you is that it's a challenge because there has been.... I don't want to be harsh on the commissioners. The commissioners are operating within the given model to the best extent they can, but there has been a regulatory failure to control this over the last years, at least since we've had PIPEDA and before the model code or at least the social media became a much stronger force in 2006-07.

It is not controlled. The question is, do we care enough about it that we want to control it and regulate it? To me, it's clear from the research—there's no way to mince words about it—that if you leave it up to individuals, they won't do much about it. But the same is true with any kind of action. If you ask me if I'm willing to pay $1 to have the police or the firefighters respond to my door faster than for somebody else, I would say no, I don't want to do that; I think they should do it as a public service.

So it all depends on the analogy you're using. It's very well possible that people just see the protection of their personal information as a right that Canadian governments, provincial or federal, should intervene on and protect, and not as something they should be paying out of their pocket to do.

Thank you.

[*Translation*]

Ms. Charmaine Borg: Do I have any time left?

The Chair: No, your time is up. The question and the answer are part of the seven minutes.

Mr. Calkins, you have seven minutes.

[*English*]

Mr. Blaine Calkins (Wetaskiwin, CPC): Thank you, Chair.

Thank you to our presenters for coming here today.

I have a list of questions. My normal monologue is followed up with a couple of questions, so I'll skip the monologue in lieu of time this morning.

Mr. Kerr, you talked about the devil in the defaults. I agree with you. Here's my question to you. Whether it's an e-commerce site where credit card transactions are being used, a social media site where a person is using a free application that's targeted for adult audiences, or a dating website, or whether these are sites that are designed for children, can we really have one set of rules that applies for protecting privacy and will cover that broad a range of user experiences and user expectations?

● (1245)

Prof. Ian Kerr: It's a great question. My short answer to that is no, but I want to start by saying that it is the current model.

The current model with PIPEDA, as with legislation worldwide, going back to the OECD guidelines on data protection in border flows, has been based on this notion of technological neutrality: that we design several key foundational principles and that those principles ought to apply across any technology, whatever technology it is. So if you look at the ten addendum points to PIPEDA—things about accountability, about consent—all of these ten principles are meant precisely to do what you just talked about, namely, to have one law that applies to all.

I'm not convinced that it will work across the board, but that having been said, I don't have the worry that I think is implicit in your question, which is that if we go down this road we're going to need to have ten laws for ten different kinds—or hundreds—of transactions online.

I do think that in the context you bring up—for example, e-commerce, social media, children's sites—the way we would design defaults in those situations would still be focused on the fair practice principles for information collection, use, and disclosure. So the defaults would be dependent upon whether and to what extent information is being collected. I do think that we will be able to study and to think carefully to define defaults that would work across a general array of technologies, the purposes of which are information collection, use, and disclosure, which are the three buzz phrases attached to PIPEDA.

I don't see particularly why that necessarily wouldn't be the case, because the defaults are around collection, so either you collect or don't collect. If you do collect, set a default that's more towards whatever the privacy context is in the particular context we're talking about.

In the same way that there are hundreds of models of automobiles, and there are motorcycles, and there are now these new electronic bikes that you see everybody puttering around the streets of Ottawa on, we haven't had that much trouble figuring out how to make speedometers for all of them. We've standardized various tools of feedback. I think we can do it here too.

Mr. Blaine Calkins: It's funny that you should mention that, because we actually do have trouble standardizing them, not within our own jurisdiction, but we have a lot of trouble when it comes to cross-border issues. Operating systems designed for whatever platform, whether it's Mac OS, Microsoft's platform, Open Source, or whatever the case might be, are not necessarily going to comply with all the boundaries.

If they're not harmonized with the international players and if we don't have our privacy laws and settings in a way that's cooperative, how do we define jurisdictional differences? For example, if the transaction server happens to be outside the jurisdictional boundaries of Canada, yet the user interface is happening inside Canada, how can we be expected to apply those laws evenly?

Prof. Ian Kerr: Right. Well, you've made the perfect case for why we need greater enforcement powers for our Privacy Commissioner, because there will be instances when companies are set up in different jurisdictions that don't have the same requirements we do.

But if we believe that there are certain standards that are baseline standards, if we believe that for Canadians, then we might need to have a different law. And guess what? Some of these companies that operate in Canada, in the same way that other kinds of businesses do, will have to comply with our laws.

Mr. Blaine Calkins: Okay. That's fair. I think most reasonable Canadians want that. I think most Canadians want their information protected. But if we create such a regulatory environment here and if we create too much of a ham-fisted or a heavy-fisted environment here, will we not be driving off our shores those same businesses and the technology and the people who want to operate in a freer environment?

Prof. Ian Kerr: Yes, I think there's a risk of that—there absolutely is—which is why we have to avoid creating these kinds of ham-fisted approaches you're talking about. What I'm talking about is really taking the principles we've already subscribed to, which are subscribed to all around the world, and operationalizing them in terms of basic defaults. I don't think it has to be at that deep level of specificity.

Mr. Blaine Calkins: I think you're right. I think defaults are where we need to start.

Mr. Levin, Mr. Gautrais, do you have anything to add to what Mr. Kerr has said in response to any of the questions I've asked? No?

I'll move on to some other lines of questioning. I was a database administrator. I was in Oracle; I looked after Oracle databases and so on. I'm not pretending I'm an expert by any stretch of the imagination in this particular field; however, I guess you could say I qualified once as an IT professional, at one point in time.

Looking after databases, particularly relational databases, particularly in client accounts dealing with particular information, there's a huge difference between deactivating something and deleting something. When it comes to the protection of people's privacy and their personal information and the right to be forgotten, I don't think we have a very explicit regulatory or legislative approach in dealing with the right of people to have their information completely removed, taken away from, or deleted from various organizations' databases.

Further complicating this, of course, is if my information has been collected during, for example, a signing on to download a free app or whatever the case might be. The information can then be resold or distributed from that point forward. I might ask the original company to delete that information; however, the damage has been done if that information has been resold. You can't trace that back.

What are some of your opinions on the concerns I've raised about being able to actually have my information taken out of a particular database if I so choose?

● (1250)

Prof. Ian Kerr: I'm happy to start. I'm not sure if the question was directed to me.

Mr. Blaine Calkins: It's to all of you.

Prof. Ian Kerr: So as a former employee of Oracle, I guess you're particularly sensitive—

Mr. Blaine Calkins: No, no, I'm not a former employee of Oracle. I want to be clear: I was an Oracle database administrator.

Prof. Ian Kerr: I see.

In any event, you will be sensitive to the famous saying by Larry Ellison, the CEO of Oracle, in the early 2000s, shortly after 9/11, that you don't have to give up any privacy; all you have to do is give up your illusions of privacy.

Voices: Oh, oh!

Prof. Ian Kerr: He was trying to sell to the United States a database so that they could implement a national identification card using biometrics, which he would then manage.

So in that context alone, and in others, I'm very sympathetic to the concerns you raise. You draw correctly an important distinction between deactivation and deletion. We in Canada will have to think more carefully about even data retention policies, because the soft version of the right to be forgotten, the right to delete—

Mr. Blaine Calkins: It used to be a matter of our not having the storage space to keep track of information, but now we're—

Prof. Ian Kerr: That's right. Storage is infinitely cheap. So it makes more sense, from a business proposition, to.... I take the same approach with my computer—

[*Translation*]

The Chair: I ask that you each provide a 30-second answer.

Dr. Vincent Gautrais: The issue when it comes to the right to forget and its application is that we face two principles recognized by the Constitution. We have to strike some sort of a balance between the two. Unfortunately, given this tendency to objectify the right to forget principle in a provision, we have more interpretation-related issues than solutions to contribute.

Once again, Europeans pounced on that principle. It cannot be applied in legal decisions. A judge could not objectify that.

[*English*]

Prof. Avner Levin: I don't think it's possible. Technologically, I think it's not possible to delete the information. We saw that just recently with that horrific video of the killing.

That's why my point in my submission was that you have to focus on how you're going to be able to use that information down the line. I think a lot of the concerns—not all of them, but a lot of them—could be addressed if you actually focused on regulating the proper use or the permissible use of that information.

[*Translation*]

The Chair: Thank you.

I will give the last question and answer period to Mr. Andrews.

[*English*]

Mr. Scott Andrews (Avalon, Lib.): Thank you.

We have three great witnesses and only seven minutes each, in a committee that started late.

I think I'll try something a little different, Mr. Kerr, so let me ask you this. We've decided for this study to bring in the Googles, the Facebooks, and the Twitters at the end of our meetings, to listen to what we've heard. If you were sitting here, what questions would you ask of them?

Prof. Ian Kerr: It's difficult to be put on the spot to answer that question, but I speak with some of the people who work with them all the time. I think one of the questions you would do well to ask is the one Madame Borg asked me previously to try to get a better sense of what exactly happens with that information once it is in their possession. I think it's really important to understand the back end of the transactions that are taking place.

I think it's also useful and important to see if we can get a sense of where these major players see things going from their perspective. I'm not clear on how much of what kinds of things they'll want to disclose if they relate too closely to their business efforts, but let me give you a quick example. Facebook in the past year or so has put forward two applications, one called Open Graph and the other called Instant Personalization. In my mind, what Facebook is trying to do is create a social graph. By that I mean the same thing as Google Street View except with each of us. So in the same way that Google Street View can take individual snapshots of each car and each house and then have this amazing technology that can seamlessly weave them together, so too Facebook wants to do that with Timeline and some of its newer applications to stitch together the fabric of our lives in order to better understand us.

So it's not just points of data on a profile, but a seamlessly integrated digital version of ourselves. I would be very interested in hearing where they are trying to go with Instant Personalization, Open Graph, and the general goal of seeking to build a social graph around us.

So that's one question for Google and one for Facebook.

● (1255)

Mr. Scott Andrews: Getting into that—because I know you did allude to it, and you wanted to come back to it when we talked about Facebook—they're going to come in and tell us everything is rosy. They are probably going to wine us and dine us with the graphs and the displays. But how do we get to the question of privacy settings? I know you mentioned you wanted to explain it, because I'm one of those Facebook users, and I remember seeing something about privacy come up at some point, but I'm too busy surfing Facebook and doing other things to go in and change those settings.

Prof. Ian Kerr: Let me tell you that you shouldn't feel too bad about yourself in that way. I recently was trying to articulate exactly how the defaults work on Facebook. I have talked about this for two years straight. I have students who live and breathe and consume the sugar of Facebook every moment, as do I, and I could not do that for you.

In order to articulate the current defaults for Facebook, we actually had to sign up a new identity and go through it from scratch, because in the past two years since I started talking about this issue, they have changed so many times which things default to friends only, which things are to friends and friends of friends, and which things are to the public. Those things are changing so frequently that I'm not surprised you haven't been able to do it. I haven't been able to do it either.

This is why I think we need some kind of a benchmark or an anchor. I think you should ask them exactly how they go about deciding whether to roll out these changes to the defaults and really what is going on there. I think you'll find what's going on there, if they answer honestly, is they want to collect more information, rather than less information. If the defaults stack towards giving them more information, they will do that. That's how they've engineered this whole thing. It just did an end run around everything our Privacy Commissioner had tried to do with them.

Mr. Scott Andrews: I remember even when you sign up for Facebook it is pretty limited. It's just your name, and your birthday is actually important—and I need to ask you why that is—and then the more you get into it the more you divulge.

It gets back to your comments regarding the contracts and the “I agree”. I scroll down and I click “I agree”.

Prof. Ian Kerr: But you don't do that because you are irresponsible. You do that because you know it's on a take-it-or-leave-it basis, and if you're using Facebook you're clicking “I agree”. If you're not using Facebook and you're a university student at a law school, you no longer have access to everything that is going on in your world; you are an outcast.

Mr. Scott Andrews: How do we get these agreements to be shorter and simpler and to require the onus to be on us as individuals to tick more of the things as “this is important” and “this is important”? And what number...? Instead of 100, is it five? Is it 50?

● (1300)

[*Translation*]

Dr. Vincent Gautrais: What is interesting is that the Facebook community has managed to get the Facebook contract changed, not regarding the confidentiality policy, but regarding the terms of use. Two years ago, Facebook changed the copyright clause, and several hundred thousand users said that we should be careful because that was bad. Facebook, which is very bright when it comes to marketing, said there was a problem and created this site that is still here today. I am talking about the “governance site”, and the elements it deals with include rights and obligations. That website was changed. The users were asked what they wanted Facebook to change in the contract, and an agreement was concluded between Facebook and the users, thus improving things.

Right now, it is impossible to influence Facebook when it comes to privacy issues. In fact, as my colleagues have pointed out, that is its fuel; it needs data to survive. It is impossible to get Facebook to change things when it comes to a contract that would.... A privacy policy, like the one Facebook has, could be written in half a page. That can be done, but they refuse to do it because they deliberately want to drown information in a lengthy policy, knowing that no one reads the damn contract.

Unfortunately, I don't think a Canadian piece of legislation will change that. I have more faith in some kind of international pressure. When I talked about informal standards, I was thinking about users themselves joining forces with international groups of all privacy commissions. Over the past two or three years, much stronger groups have been formed—and the Office of the Privacy Commissioner of Canada is part of them—which may try to influence a policy through negotiation in order to achieve a contract that is legible, reasonable, and half a page in length at the most.

The Chair: Unfortunately, the time is up, and I must interrupt you. I know that it is already 1 p.m. and we will have to adjourn the meeting very soon.

Just before we go, I would like to mention that, next Thursday, there will be no meeting, since we will likely be voting. If I have the permission, we will summon the witnesses who were supposed to appear on the 14th to come on June 21. Therefore, they will come on Thursday, June 21, instead of Thursday, June 14, since we will be voting. I think that this will work for everyone. We had nothing planned on Thursday, June 21. So that works for everyone.

On that note, I want to thank the witnesses for joining us today, although we did not have as much time as we would have liked. We may see each other again eventually. Thank you.

The meeting is adjourned.

Published under the authority of the Speaker of the House of Commons

SPEAKER'S PERMISSION

Additional copies may be obtained from: Publishing and Depository Services
Public Works and Government Services Canada
Ottawa, Ontario K1A 0S5
Telephone: 613-941-5995 or 1-800-635-7943
Fax: 613-954-5779 or 1-800-565-7757
publications@tpsgc-pwgsc.gc.ca
http://publications.gc.ca

Also available on the Parliament of Canada Web Site at the following address: http://www.parl.gc.ca

Publié en conformité de l'autorité du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

On peut obtenir des copies supplémentaires en écrivant à : Les Éditions et Services de dépôt
Travaux publics et Services gouvernementaux Canada
Ottawa (Ontario) K1A 0S5
Téléphone : 613-941-5995 ou 1-800-635-7943
Télécopieur : 613-954-5779 ou 1-800-565-7757
publications@tpsgc-pwgsc.gc.ca
http://publications.gc.ca

Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante : http://www.parl.gc.ca