House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 029 • 1st SESSION • 39th PARLIAMENT

EVIDENCE

Thursday, February 8, 2007

Chair

Mr. Tom Wappel

Standing Committee on Access to Information, Privacy and Ethics

Thursday, February 8, 2007

● (0900)

[*English*]

The Vice-Chair (Mr. David Tilson (Dufferin—Caledon, CPC)): Good morning, everyone. We're a few minutes late, so I'd like to start.

This is the Standing Committee on Access to Information, Privacy and Ethics, meeting number 29. The orders of the day are pursuant to the order of reference of Tuesday, April 25, 2006, section 29 of the Personal Information Protection and Electronic Documents Act, a statutory review of the act.

[*Translation*]

Mr. Robert Vincent (Shefford, BQ): I have a point of order, Mr. Chairman. I would like to know something.

[*English*]

The Vice-Chair (Mr. David Tilson): You may have two seconds, sir.

[*Translation*]

Mr. Robert Vincent: I would like to know how many people we need for quorum at the committee.

[*English*]

The Vice-Chair (Mr. David Tilson): We don't need a quorum to start the meeting. I'd be prepared to oblige, but if members aren't here—

We were supposed to start at 9 o'clock, and people drift in. So we're entitled to start.

[*Translation*]

Mr. Robert Vincent: That's fine; I have no problem with that.

[*English*]

The Vice-Chair (Mr. David Tilson): The only problem would be if there were a vote, and there is no vote, unless someone is up to something.

We have two guests today: IMS Health Canada, of which Anita Fineberg, I trust, is the spokesperson; and the National Association for Information Destruction - Canada, and I assume Dave Carey is the spokesperson.

Ms. Anita Fineberg (Corporate Counsel and Chief Privacy Officer, Canada and Latin America, IMS Health Canada): I'll be speaking with Gary Fabian.

The Vice-Chair (Mr. David Tilson): Thank you.

We allow up to 10 minutes for each group to have some introductory comments, and then members of the committee, I expect, will have questions for you.

I want to thank you all for coming and providing us with your comments.

We will start with you, Ms. Fineberg, if you could introduce your colleagues.

● (0905)

Ms. Anita Fineberg: Certainly. As you mentioned, I'm Anita Fineberg. I'm the chief privacy officer and corporate counsel of IMS Health for Canada and Latin America.

With me this morning is Gary Fabian, the company's vice-president, public affairs and government relations.

Also with me is Dr. Léo-Paul Landry, a member of our national medical advisory board and a past CEO and secretary general of the Canadian Medical Association. Dr. Landry brings the physician's perspective to the issue we'll discuss today and has particular experience and expertise in the province of Quebec.

I'd like to first thank the committee for providing IMS the opportunity to appear before you today. With the committee's permission, Gary will first provide you with some information on our IMS business, what we do, the data we collect, and our contribution to the advancement of health; and then I'll explain the impact that PIPEDA has had on our business and why we're here today.

Mr. Gary Fabian (Vice-President, Public Affairs and Corporate Relations, IMS Health Canada): Good morning. My name is Gary Fabian. I've been associated with IMS Health for over 20 years in a variety of roles. As vice-president of public affairs, I work closely with the medical, pharmacy, and research communities across Canada, primarily in a collaborative fashion, around the optimal utilization of medications.

IMS Health is the world's principal provider of information, statistical research, and consulting services to the pharmaceutical and health care sectors. We track over one million products globally, helping health care stakeholders to implement evidence-based decision-making.

We've been operating our business in Canada since 1960. Our Canadian head office is in Montreal, where we have over 850 employees. We have another office in Toronto with over 85 people, and a small office in Edmonton, Alberta.

We collect data from over 6,500 sources in Canada, including hospitals, pharmacies, pharmaceutical manufacturers, wholesalers, and physicians, to yield extensive information on diagnoses and disease treatments, including prescribing patterns and pharmaceutical utilization trends.

We maintain the most comprehensive national prescription database in Canada. Essentially, we have any and all information related to pharmaceutical distribution, consumption, and use in Canada, with one very important exception: we do not collect, use, or disclose any identifiable patient information; therefore, patient privacy is never at risk. We go to great lengths to ensure that patient privacy is always protected.

The facts are that since our Canadian operation began in 1960, we have never experienced a breach of patient privacy. We have never received a complaint from a patient that their privacy has been compromised. We have never received a complaint from a patient that their relationship with a physician has been jeopardized or compromised in any way. We have never received a complaint from a physician that their relationship with a patient has been compromised or jeopardized. This is the reality as opposed to unsubstantiated speculation.

[*Translation*]

We provide information products and services to governments, researchers, health providers, regulators and the private sector—pharmaceutical and biotech companies—to support the safe and effective use of medications, evaluation of drug policies, implementation of best practices and economic analyses. Physician-led research has used IMS data to measure the impact of continuing medical education initiatives on prescribing practices. Quality improvement initiatives for the use of antibiotics in Alberta and B. C., the development of new prescribing guidelines for Ritalin to children in Quebec and a long-term study examining the use of psychotherapies for depressive disorders associated with multiple sclerosis currently being conducted in western Canada have all benefited from the use of IMS data. It is our paying commercial clients that have enabled us to develop and invest in the production of the timely, up-to-date information available and to provide it gratis to help researchers.

On the government side, we provide data to the Patent Medicine Prices Review Board to assist with their previous setting of prices for brand drugs, and currently for the monitoring of the prices of generic drugs in Canada. Health Canada is also an important client of IMS and uses our information to assess current drug legalization trends and to develop health policies. Other government departments, federally and provincially, frequently use IMS expertise for similar reasons.

We are counselled by a medical adviser board comprised of three prominent physicians: Dr. Léo-Paul Landry, who is here with us and represents Quebec, Dr. Bill Orovan, representing Ontario, and Dr. Larry Olhauser, representing the western region. We interact with numerous physician-researchers in several academic settings, such as universities and other health research centres of excellence.

Our data is neutral—that is, we do not make judgments on whether the use of a particular therapy is good or bad—it is used by others to support evidence-based medicine and to make policy decisions in critical areas such as controlling drug costs, assessing utilization trends and the development of prescribing guidelines. Our objective is to ensure that we have the most comprehensive, valid and timely data available to support evidence-based decisions.

● (0910)

[*English*]

Ms. Anita Fineberg: I've been IMS's chief privacy officer since 2000. We were one of the first companies in Canada to have such a position. I joined the company from the Ontario Ministry of Health, where I provided legal advice to the ministry on all privacy-related issues under the provincial public sector privacy and access law. I previously worked at the Information and Privacy Commissioner's office in Ontario for a number of years. So my experience in privacy and access issues spans the government, the regulator, and now the private sector.

You'll recall that Gary referred to one of IMS's key databases, information we receive from pharmacies that identifies drugs that have been prescribed by identified physicians. I again emphasize that we receive no patient identifiable information. We do not have access to the actual prescription record. Information that we receive about physician prescribing practices is disclosed in groups of at least 30 physicians. Generally, the groups are much larger. So that the actual prescribing pattern of an individual physician is never disclosed, rather a client sees a report that indicates one number for all the named physicians in the group.

Physicians may have access to their individual prescribing information upon request to IMS. It's free. IMS only discloses the information on an individual basis to the physician or as required by law.

Why are we here today? We're here to request that the committee consider a narrow technical amendment to PIPEDA to clarify, codify, and provide certainty that work product information be excluded from the definition of personal information and therefore from the scope of the act.

As the committee knows, the definition of personal information in PIPEDA is information about an identifiable individual. The definition then goes on to exclude the name, title, or business address, or telephone number of an employee of an organization. The question is whether the information IMS receives from pharmacies related to a physician's prescribing is subject to PIPEDA.

When the legislation was being drafted and debated, we had questions as to whether the apparently very broad scope of the definition would capture the prescribing information, which did not appear to be intended. Even before the act came into force, our data suppliers and our clients expressed concerns about the information because of the lack of clarity in PIPEDA. As soon as the act came into effect in 2001, we were advised by the commissioner's office that they had received two complaints about our practices, alleging that we were contravening PIPEDA, as we were collecting personal information without the consent of physicians.

In the fall of 2001, the commissioner issued his findings on both complaints together, concluding that the prescribing information is not personal information, but rather work product information, and thus not subject to PIPEDA.

One of the complainants, a former business competitor, took the matter to the Federal Court, where it was dismissed, on consent of all parties, in the spring of 2004.

Working with Industry Canada, we proposed that a clarifying regulation be promulgated under PIPEDA to ensure the legislative intent that such information was not subject to the act was clear. However, the Department of Justice provided the opinion that such clarity had to be provided through a legislative amendment as opposed to a regulation. We followed their advice, so we're here today asking for such an amendment.

Why is it necessary? We, and others that you've heard from, still operate under a cloud of business uncertainty. Despite the commissioner's finding, another complaint against IMS on the same question could be filed with the commissioner's office tomorrow. As you've heard, the commissioner could make a different finding. She has no obligation to follow the previous one. As you can appreciate, this is a very difficult and uncertain environment in which to conduct business and to make decisions about ongoing investments in technology, infrastructure, and human resources in our Canadian operation in Quebec, Ontario, and Alberta.

Just as importantly, in the Canadian privacy environment, we've seen over the years an explicit recognition of the commissioner's finding on work product. You've heard from Department of Industry representatives that B.C. has substantially similar provincial private sector legislation, PIPA. This came into effect in January 2004 and, in effect, codifies the commissioner's finding. It has a definition of work product information that's explicitly excluded from the definition of personal information.

● (0915)

The Vice-Chair (Mr. David Tilson): Ms. Fineberg, you're in excess of 10 minutes. Perhaps you could wind up soon, please.

Ms. Anita Fineberg: Certainly.

You've heard from many witnesses who have appeared before you today who support a specific exclusion for the definition of work product information: David Loukidelis, the Privacy Commissioner of B.C., who indicated that the definition in B.C. has not created any concerns; Edith Cody-Rice and Don Brazier, on behalf of FETCO; the Canadian Bar Association and its summary of proposed amendments, submitted to Industry Canada; and the Insurance Bureau of Canada and CLHIA.

A work product exclusion, which we have proposed as an amendment on the last page of our submissions, builds on that in the B.C. legislation. It addresses potential concerns, identified by the federal commissioner and Professor Bennett, with respect to the interpretation that might put employee surveillance activities outside the scope of the act. It's broad enough to capture many types of work product information identified by witnesses before the committee, and it's narrow enough just to exclude the type of work product information that witnesses have agreed is qualitatively different from personal information, which should be afforded privacy protection under the act.

The Vice-Chair (Mr. David Tilson): Thank you.

Mr. Carey, it's your turn.

Mr. Dave Carey (Chair, National Association for Information Destruction - Canada): Thank you. I'm Dave Carey, vice-president of Iron Mountain Secure Shredding, and the elected volunteer chair of NAID Canada. With me is Robert Johnson, the executive director of NAID and NAID Canada.

On behalf of the National Association for Information Destruction, NAID Canada, I would like to thank the committee for the opportunity to speak here today.

NAID Canada is a non-profit trade association for the secure information destruction industry. NAID Canada's members, like those of its sister organizations in the U.S. and Europe, provide commercial services ranging from the secure shredding of discarded paper records to the destruction of information contained on end-of-life electronics.

We take the invitation to address you here this morning as a sign of a growing understanding among policy-makers around the world that protecting personal information at the end of its life cycle is every bit as important as protecting it during its useful life. We will offer recommendations to reflect that in the legislation.

NAID Canada and its sister associations in the other countries have earned a reputation as a vigilant consumer advocate and as a trusted and credible resource for policy-makers. Our association has been asked to provide counsel in matters of proper information destruction to the Canadian Privacy Commissioner's office; the Ontario Information and Privacy Commissioner; the governments of Ontario, Alberta, and British Columbia; the U.S. Federal Trade Commission; the U.S. House of Representatives financial services committee, and the British Standards Institute.

With that said, we did not travel here today simply to remind you that discarded personal information should be destroyed first. That is a basic and well accepted principle of information protection. However, we would like to share with you our observation that governments need to provide a higher level of direction to ensure compliance with this principle and thereby real protection for its citizens. We maintain that you have that opportunity by amending PIPEDA.

Even with PIPEDA and other applicable provincial regulations in place, personal information is routinely abandoned or discarded without benefit of proper destruction. Here are a few examples.

In September 2005, a film company obtained several hundred boxes of office paper from a recycling centre to be used to replicate the scene of the World Trade Centre tragedy. As it turned out, the recycling company had delivered confidential medical records to fulfill that request. These most personal records were then summarily strewn about the windy city streets of Toronto's business district.

Most recently it was widely reported that bank employees had deposited confidential information in publicly accessible waste bins. The resulting investigation found the bank had inadequate policies and procedures to ensure proper information destruction.

In March 2006, a B.C. government official sold magnetic tapes at public auction that contained 77,000 medical files, including those of patients with many sensitive diagnoses. A month later, in Winnipeg, the dental records of hundreds of citizens were reported to have been found in a dumpster.

The truth is that these incidents are unique only in that they made the headlines. On any given day, it would not take long to find personal information being discarded, intact and accessible to the public. Careless disposal in dumpsters or garbage bins is the obvious example. Keep in mind as well, however, that recycling alone is not safe information destruction. Documents may still remain intact and vulnerable to privacy breaches for extended periods of time before being recycled.

Privacy protection is no longer simply a human rights issue. Violating the rights of others by casually discarding their personal information provides much of the feedstock for what has become a global epidemic of identity fraud. According to a study conducted in the United States, the vast majority of identity theft results from low-tech access to personal information such as dumpster diving. Indeed, law enforcement officials in the U.S. recently exposed elaborate rings of organized criminals capitalizing on this ready source of personal information. These rings were found to have divisions of labour, where lower ranks start by harvesting the information from dumpsters, which is then handed over to others of higher rank who have been trained to exploit it.

Only in the United States has a new generation of legislation begun to appear, exemplified by FACTA and a host of state laws. It is designed not only to protect privacy rights, but also to stem the tide of identity fraud. As a result, there is a marked difference in the regulatory language regarding information disposal.

● (0920)

Where in the past a regulatory reference to information disposal would require limiting unauthorized access, improved regulations now require that steps be taken to destroy personal information prior to its disposal. Further to the point, the newer generation of legislation requires that such security measures be documented in the organization's policies. We are here to respectfully urge this committee to enhance the effectiveness of PIPEDA in protecting the citizens of Canada by adopting a similar approach. Information destruction requirements must be clearly spelled out in legislation. That is the only way to put an end to these unnecessary breaches.

A number of specific recommendations must be noted to ensure that such protections are effective. We will focus on the most important here.

To ensure the full impact of a requirement to destroy discarded personal information, NAID Canada recommends that information destruction be clearly defined as “the physical obliteration of records in order to render them useless or ineffective and to ensure reconstruction of the information, or parts thereof, is not practical”. Enshrining such a definition is critical. It cannot be left to interpretation, as it is currently.

Further, we recommend that any organization that collects or stores personal information must have an information and document destruction policy. That forces organizations to think about the issues and implement a policy that fits the definition just provided.

We also support stronger contracting requirements between information custodians and third parties to whom processing is outsourced. That contract should clearly delineate the third party's responsibilities, policies, and procedures. The contract should also clearly indicate the third party's acknowledgement that they are bound by the same obligations as primary custodians to protect the personal information under PIPEDA.

We also recommend requiring information custodians to provide notification to individuals put at risk by breaches of security. Historically, such notifications have been reserved for incidents involving sensational electronic data breaches. However, just over a year ago there was an incident where millions of citizens of Los Angeles were put at risk by irresponsible disposal of paper records. In that case, L.A. County determined that the incident warranted a formal notification event. It is our recommendation that PIPEDA not only be amended to include a notification requirement for electronic data put at risk, but also casual disposal of paper records.

In closing, everything we have recommended this morning is already included in current information protection regulations elsewhere in the world. Identity theft is a growing scourge with no borders. When governments strengthen information protection in one jurisdiction, the criminals will move to where the laws are weaker and less well defined. Also, keep in mind that as processors of personal information ourselves, we fully understand that we are subject to the same regulations and consequences of violation.

Finally, I will leave you with a story that best demonstrates the value of increased government direction in the area of disposal. In May 2002, the State of Georgia passed the first serious shredding law in the United States. About two weeks afterwards, our executive director received a call from the VP of operations of a very large insurance company, well known to everyone in this room. The gentleman asked if NAID could send him a list of our NAID members in Georgia so that their multiple claims offices could comply to that new law. Of course, we were more than happy to accommodate the caller, but our director added that he could also send a list of NAID members across the country for their other offices. Without a second thought, the customer said, no thanks, the other states don't have a shredding law.

I wish I could tell you that your good counsel and prodding would be enough to prevent the casual disposal of personal information. But history has proven that more deliberate direction is required. Most importantly, the legislation must define the term “information destruction”.

Thank you for the opportunity to appear here today. We remain at your service at any time to provide further input or support for this committee's efforts to better protect the privacy of Canadians. Thank you.

● (0925)

The Vice-Chair (Mr. David Tilson): I want to thank you and all our guests for coming and making your presentations to us.

I know members of the committee will have some questions, and in the procedure we follow, we go in rounds. The first round is up to seven minutes for questions and answers.

We will start with Mr. Pearson.

Mr. Glen Pearson (London North Centre, Lib.): Thank you, Mr. Chair.

Thanks for coming today, and for updating us on this.

My question is for Ms. Fineberg.

We keep hearing at these sessions over and over again of the distinction between personal information and work product information, so we understand that there's a distinction there, and we also understand that the Privacy Commissioner also recognizes that distinction. But it does seem to me that distinction gets pretty murky when you start saying that it can be decided on a case-by-case basis. I understand that gives some people some comfort. On the other hand, if you are a business it's very difficult to plan for the long term.

I would be interested in knowing your view on that. Also, in your particular field of work and what you're doing, how does this affect your long-term planning?

Ms. Anita Fineberg: Thank you.

I think the difficulty with the case-by-case approach proposed by the commissioner is that it really doesn't give any legislative policy direction, as determined by Parliament, to the commissioner to interpret any individual case. In that situation, policy would effectively be left up to the commissioner, as opposed to the commissioner being required to apply the policy that government and Parliament had determined. I think it's particularly important in this case, when we're talking about the definition of personal information versus work product, because of course that definition determines whether the information is subject to the rules of the act—whether you're in scope or without scope.

As for how that would impact our company particularly, the case-by-case approach doesn't provide any long-term certainty for anybody. As we've mentioned, a complaint tomorrow could be decided differently. The Federal Court could ultimately decide differently as well.

On our data that's used for long-term research projects, you want to look at trends over time precisely because they're long-term projects. Again those projects require certainty that you're going to be able to continue collecting data from your population at issue.

The commissioner appeared to indicate she has accepted that there's a qualitative distinction between personal information and work product, so it's kind of difficult to understand why that policy direction should not be clearly provided in the legislation itself, as it has in the B.C. legislation, for example.

● (0930)

The Vice-Chair (Mr. David Tilson): Mr. Vincent.

[*Translation*]

Mr. Robert Vincent: My question is for Ms. Fineberg and I also have one for Mr. Landry.

In your brief, you state: We are here to request that the committee consider a narrow, technical amendment to the PIPEDA, to clarify, codify and provide certainty that "work product information, be excluded from the definition..."

First of all, what is your interest in seeing the prescriptions?

Second, if we amend the act regarding doctors' prescriptions, any insurance company will be able to get access to these prescriptions. Would there not be a link between these two things?

Mr. Gary Fabian: We try to make a distinction between the two. The work product, in our view, has no information about the patient. That is the distinction that we make. The information available is what is contained in the prescription, that is, what the doctor has prescribed. However, the federal commissioner has ruled that this information is not personal information.

If the prescription contains personal information about the patient, that would obviously be different. But since we have no access to the prescription as such, we cannot get any information about the patient. That is the distinction that we are trying to make by talking about the work product.

Mr. Robert Vincent: All right. However, if we amend the legislation, anyone could use it. If we say that prescriptions are a work product, an insurance company could ask the physician of the victim of a highway accident or some other mishap to consult that person's medical file. In that way, they would be able to see what other medications have already been prescribed to that person for a back problem, for example. That would allow the insurance company to say that this person already had issues with his back, and that consequently, the accident is perhaps not the cause of his current back problem.

Would it be possible for someone to use that information for means other than those you recommend?

[*English*]

Ms. Anita Fineberg: In the example you provided, the medical record would not include any information about the patient, or the individual in your example who was in the accident, suffering back pain. We would not know—nor would the definition we propose for work product cover anything that would identify the patient, or the accident victim in that particular case.

What we are talking about, to use an example that many witnesses have provided to the committee, are things like documents, memoranda, opinions, and correspondence that are authored by people as they function as employees or professionals in an organization. It wouldn't include personal information about somebody, like their medical condition, religious beliefs, or something removed from that, reflecting, "I went on a call report to try to sell my company's clients a widget. I came back and wrote a report for my manager about that encounter and how many widgets they wanted to buy, and how many they didn't want to buy." We're talking about that report as a work product of the salesperson who wrote it. That's the type of information we are proposing should be explicitly excluded as a work product in PIPEDA.

[*Translation*]

Mr. Gary Fabian: The information we have about a doctor would not be personal either, because it is truly a work product. The person's religion, salary, preferences, habits or the kind of car they drive would not be information we would have access to, because that is personal information.

● (0935)

Mr. Robert Vincent: I understand your point of view and I agree with what you are asking for.

Let's take a concrete example. Someone slips in your yard and files a claim for a redemption or benefit. I know you are talking about more significant amounts than that. If one says to the doctor that this is not personal information because it is a work product, I am afraid that the insurance company could turn to the treating physician and say that it is a work product. It is decriminalizing it in a sense, and it could be used in that way.

Dr. Léo-Paul Landry (Member, Medical Advisory Board, IMS Health Canada): Mr. Chairman, may I answer?

Generally speaking, in a hospital environment, the situation is relatively simple. If a person suffers an injury during an accident or some kind of incident and the company asks for a medical report in order to study the situation, it is in the interest of the person who was injured, who was wounded or was in an accident to give his authorization. That is how things happen 99.9% of the time.

This poses a problem when the opposing party asks for information and the injured party refuses to disclose it. Normally, this is settled by both parties' attorneys. Generally speaking, this does not pose a problem.

Mr. Robert Vincent: The insurance companies are asking us the same questions and tackling the same aspects. Should the prescriptions that are work products that we are discussing here not be the subject of excessive scrutiny or be considered as personal information? If that is the case, is it so that doctors could consult an injured person's file and see the prescriptions? If we say that this information is a work product, these documents are not confidential. I want to see my way clearly in this.

Dr. Léo-Paul Landry: It is difficult to respond to each of the aspects you have raised. We have not studied this issue and we have not heard the industry's comments. Personally, I cannot answer you.

Mr. Robert Vincent: All right.

Dr. Léo-Paul Landry: All I can tell you is that we, at IMS Health Canada, do not have access to patient files and we do not want to have access to them. We cannot talk about 100% because there are always exceptions, which by the way are covered by the act, but in 99.999% of the cases, we use the information generated by what we call the work product in the doctor-patient relationship in order to improve services to the population without knowing the identity of the patient.

Mr. Robert Vincent: In your case—

[*English*]

The Vice-Chair (Mr. David Tilson): Thank you. That will have to wait until the next round, Monsieur Vincent and Dr. Landry.

Mr. Martin.

Mr. Pat Martin (Winnipeg Centre, NDP): Thank you, Mr. Chair, and my thanks to the witnesses.

I'm going through the IMS documents. I'm sorry I wasn't here for the actual presentation, but I've scanned the presentation.

I'm interested in a couple of general things that are beyond your brief. The duty to notify, of course, keeps coming up in our work here as a committee. We're rapidly approaching the end of the study on PIPEDA and we'll be making recommendations, so I would appreciate a brief comment from both of the witnesses as to how they feel about that.

The other thing is the transborder transfer of information. There are some jurisdictions that will not allow the transfer of data to jurisdictions that don't have comparable protections. That would be of interest to me too.

Specifically on IMS, Ms. Fineberg, I notice that on page 3 of your speaking notes, you say your business is to "provide information products and services to governments, researchers, health providers, regulators and the private sector—pharmaceutical and biotech companies—to support the safe and effective use of medications", and so on. Is there ever a case in which the pharmaceutical and biotech companies want to know from you not personal information but information regarding frequency of claims of certain types of drugs or the experience of certain types of treatments in certain jurisdictions, so that they can have an idea which products are more popular, which are being used, etc.? Is that one of the information services you might offer to the pharmaceutical and biotech industries?

● (0940)

Ms. Anita Fineberg: I'll let my colleague Gary Fabian answer that one.

Mr. Gary Fabian: One of the fundamentals of our database, because it's so comprehensive and spans the country, is that we're able to provide the research community, the pharmaceutical sector, and governments as well, with comparative data. Exactly the kind of analysis that you're talking about can be done fairly readily. It can be done by province or even by areas within a province, to allow for that kind of comparison in order to see if there are differences in a certain area versus another area.

Mr. Pat Martin: What if the same question was asked not just for medical and scientific purposes, but for commercial interests?

Mr. Gary Fabian: For the pharmaceutical sector, it's also important. They want to know where their drugs are being dispensed, for what reasons if possible, and whether there are differences in different parts of the country. That's all information that's important for them as they try to evaluate the efficacy of their own performance or their own drugs.

The Vice-Chair (Mr. David Tilson): Mr. Carey, I think the first couple of questions may have applied to you. Do you have any response?

Mr. Dave Carey: Which ones would—

Mr. Pat Martin: The duty to notify and the transnational or transborder transfer of information.

Mr. Dave Carey: I'll let Robert take that.

Mr. Robert Johnson (Executive Director, National Association for Information Destruction - Canada): Thank you for the question.

First of all, on notification, from our comments, NAID Canada's position would clearly be that notification is not only important as a protection for the individual whose information may have been breached, but I think we all know that as much as teeth or enforcement can be put into this, it may be one of the most serious deterrents to casually treating the information as well. If notification is hanging out there as an obligation, I think you're going to see organizations that handle personal information be much more concerned about that real thing happening.

As far as the transborder issue is concerned, it has cropped up. It originally cropped up when the European Union adopted data protection directives and then directives about sharing that data with the U.S., which was lagging behind at that time. It has also arisen between Canada and the U.S. with regard to the Patriot Act being passed in the U.S., and various things like that.

I would just say that it is fairly common-sense. As far as NAID Canada is concerned, the common-sense approach would certainly be that personal information belonging to a jurisdiction's citizens should not be allowed to be shared or to enter into an environment where those same protections aren't allowed for in the other jurisdiction.

Mr. Pat Martin: That's very useful to us, because we actually contracted out the gathering of our census information to Lockheed Martin recently, and that was the big issue. It eventually didn't happen, I believe, but our concern was the Patriot Act.

If we did put rigid cross-border or transborder limitations in effect in our recommendations now, that could effectively halt the flow of an awful lot of information to the United States, couldn't it?

Mr. Robert Johnson: If I may, it has generally been approached through safe harbour mechanisms that are negotiated even within... perhaps not the U.S., but within the organization. Obviously if the U. S. were to have a law that trumped that or exempted that safe harbour agreement, that would be an issue as well.

Mr. Pat Martin: On safe harbour, though, if the information isn't in Canada and the information isn't in the States, but it's in some safe harbour, then where is it?

Mr. Robert Johnson: Let me explain what I mean by safe harbour. For instance, with the flow of information from Europe into North America, after the data protection directives passed, the Federal Trade Commission, along with the EU panel working on that, developed a process by which companies could ascribe and self-certify to meet certain standards that made them, in particular, compliant with the data protection directives.

Mr. Pat Martin: They stipulate themselves to a certain set of guidelines.

Mr. Robert Johnson: Exactly.

Mr. Pat Martin: But that would fall short of any statutory legislation and there wouldn't be any punishment for compliance. Who would enforce that then?

Mr. Robert Johnson: It falls to a commercial entity. For instance, in Europe, there was a time when United Airlines was not allowed to fly into Switzerland for about two hours because they had collected data that the data protection directives said it was unnecessary to collect.

Also in Switzerland, I think, Coca-Cola was shut down, or had the threat of being shut down, because Coca-Cola was collecting more information than it needed to. The only enforcement the Swiss could do against the multinational corporation was to say the corporation was not going to operate in their country if they were not going to comply with Swiss—

● (0945)

Mr. Pat Martin: That would smarten them up pretty quickly, though.

Mr. Robert Johnson: It worked very effectively.

Mr. Pat Martin: I think Ms. Fineberg wanted to add something. Do I have a small window—

The Vice-Chair (Mr. David Tilson): If it's very brief, you have about 15 seconds, Mr. Martin.

Ms. Anita Fineberg: On the transborder issue, we have no personal health information stored in the U.S., but I'd refer the committee to two orders of the federal commissioner dealing precisely with that issue. She has ruled that contractual mechanisms between a company in Canada that outsources the data—

The Vice-Chair (Mr. David Tilson): I think it's actually in the act.

Ms. Anita Fineberg: It is, and she's ruled that to be sufficient when somebody has objected.

The Vice-Chair (Mr. David Tilson): Thank you, Ms. Fineberg.

Mr. Stanton.

Mr. Bruce Stanton (Simcoe North, CPC): Thank you, Mr. Chair.

My thanks to our panel for attending this morning. With just seven minutes, I'm going to divide as equally as I can here, because I do have two questions for each of the two groups represented here.

First to Ms. Fineberg, I'm actually referring to the recommendation that you have put on page 34 of your submission, which is the actual text of what you're proposing in relation to your work product information and how to include that as an exception to the definition of personal information.

Specifically, in your second recommendation, which talks about the definition of work product information, subsection (i) says that work product information "does not include—personal information about an identifiable individual who did not prepare, compile or disclose the information", and then it goes on to talk about the surveillance issue. It's good that you see the surveillance issue covered.

My question really is, from a practical point of view, who are we really talking about here? Could you give me a practical example of who would be excluded here?

Ms. Anita Fineberg: Since we've mentioned and you've heard about the prescription issue or the medical record issue, I'll use that, if I might, to illustrate what we're talking about in the first section.

For example, say you have a prescription. That's information that was prepared by a physician, but if it has identifiable information in it about the patient—the patient's name is still in it—that part is personal information about an identifiable individual, the patient, who did not prepare, compile, or disclose it. So if both parties are identified—the preparer of the document, meaning the physician, and the PI, meaning the personal information, about the subject—

Mr. Bruce Stanton: The patient.

Ms. Anita Fineberg: —the patient, yes—it is not work product, so the information is not excluded.

To get back to the same example, where none of the patient identifiers appear and it's again the physician who has prepared it, then it becomes work product information.

Mr. Bruce Stanton: If I can summarize, then, work product information effectively includes, for example, reports and other materials prepared by individuals or groups in the course of their profession, but if there's some personal information embedded in that —

Ms. Anita Fineberg: Correct.

Mr. Bruce Stanton: —it would still be considered personal information.

Ms. Anita Fineberg: That's right, if it's about another individual. That's correct.

Mr. Bruce Stanton: You mentioned that although there have been judgments by the Office of the Privacy Commissioner as well as by the Federal Court, your concern is that without getting this clarification, there could be another complaint that could in fact lead to the commissioner's taking a different view.

What is the commissioner's track record on these types of issues? Has she—or he, in the past—given any indication that precedents have not been followed in these types of cases?

Ms. Anita Fineberg: If I might clarify a couple of things with respect to this particular issue, there was the finding on the complaints in the IMS situation of the previous commissioner. The Federal Court did not rule on that; it was dismissed on consent of all parties.

Then last year a finding was issued by the commissioner's office, not on this particular type of information but on information related to real estate agents. The finding in that particular case was that the information at issue was in fact personal information. As a result of that, a number of commentators said this must have overruled the IMS decision, so IMS's practice—

● (0950)

Mr. Bruce Stanton: I don't want to cut you off, but I just want to keep going here. Thank you very much.

Mr. Carey, the direction you're heading in would be very good for your industry, and I think we get the point there. Do you have any knowledge to suggest that any of the breaches you described were in fact brought before the Privacy Commissioner in terms of a complaint?

Mr. Dave Carey: Yes. Rob, do you want to touch on the exact details?

Mr. Robert Johnson: Without getting into each individual case, I can tell you that each of them was handled at the provincial level through the provincial privacy and information commissioners; investigations were conducted, and results are either pending or have been produced in all of these cases.

Mr. Bruce Stanton: Were these breaches, then, in Alberta, B.C., or Quebec?

Mr. Robert Johnson: They were in Ontario. The movie set incident happened in Toronto.

Mr. Bruce Stanton: Did that have to do with the health records?

Mr. Robert Johnson: Those were the medical records that were spread around the streets.

Mr. Bruce Stanton: Would you consider that the recourse in those breaches that were followed through was somehow not sufficient? What I'm driving at is that PIPEDA already includes prohibitions against this kind of release of personal information. It is inherent in the act now that organizations that have personal information are required to protect it, and how they go about protecting it—whether they destroy it when they're finished with it, and so on and so forth—is their responsibility, but you're suggesting we have to lead them by the hand and tell them what they actually have to do with it. Why do you think the current responsibilities of these organizations are not sufficient?

Mr. Robert Johnson: I would say that while there is direction provided already, as you acknowledged, we are asking, just as you've said, for a clearer direction saying specifically that it must be destroyed when it's discarded and describing what that destruction is, along with the other recommendations. The reason is that the current level of direction falls short of what has been found to be necessary throughout much of the world to actually get action to be taken. As we've pointed out, in these high-profile cases—they were rather high-profile and made headlines—the reality is that this is happening very much as standard operating procedure, unfortunately, and it's so commonplace that it's not reported. As a result, the current statute, as it is written, is largely disregarded.

Mr. Dave Carey: We feel the number of breaches and the degree of the breaches would be limited and would decrease under better legislation.

The Vice-Chair (Mr. David Tilson): Thank you, Mr. Stanton.

That concludes the first round. We're now into five-minute rounds.

We'll begin with Mr. Dhaliwal.

Mr. Sukh Dhaliwal (Newton—North Delta, Lib.): Thank you, Mr. Chairman.

I also wish to thank the panel for coming.

As Ms. Fineberg mentioned, in your business there was not a single breach in protecting privacy and private information. On the other hand, some people are saying that the search could be narrowed down to a patient or a doctor. What is your view about that particular case, when it comes to work product and personal information?

Ms. Anita Fineberg: Certainly on the personal information side, IMS has been a very strong supporter of patient privacy rights. When there was a suggestion that the information we have might be identifiable in some way, I would say to people that clearly it is illegal across the country for IMS to collect, use, or disclose any identifiable patient information without that individual's consent. We have lots of measures in place to ensure that we do not do that.

There was a previous witness, I believe it was Dr. Rosenberg, who suggested that based on some work that was done a number of years ago in the U.S., perhaps people could be identified through publicly available information. The situation down there is very different. They don't have the privacy laws that we do, the federal Privacy Act and provincial laws that prohibit the availability of databases, such as our voters lists, motor vehicles licensing databases, vital statistics, and so on. As a matter of fact, a researcher up here in Ottawa recently tried to replicate those U.S. studies and found that it was not possible to do so. If the committee likes, I can provide that reference afterwards.

As I mentioned, we've never had a breach of patient privacy. With respect to physician information, as a matter of fact, we have had a code of practice in place for a number of years that sets out explicitly how we deal with all this information. We are transparent; it is posted on our website. It has been there for a number of years, and it's based on the Canadian Standards Association's principles, which is the code that is a schedule to PIPEDA.

Also we're independently audited each year by QMI, which is an audit branch of CSA. Our most recent certification is in your packages.

● (0955)

Mr. Sukh Dhaliwal: On the other issue, we keep hearing that B. C. and Quebec have their own legislation that is much better than PIPEDA. What is your view?

Ms. Anita Fineberg: As a matter of fact, on the provincial level, it's B.C., Alberta, and Quebec that have substantially similar legislation. I believe that what the committee has heard to date is that B.C. and Alberta represent what the commissioner called the second generation of privacy laws, and that perhaps we should take some direction, based on the learnings over time and how those provinces have accommodated them.

I also believe that when the commissioner was here, Vice-Chair Tilson specifically asked her if there were particular things in the Quebec legislation that she might suggest should be incorporated into or looked at for PIPEDA. I recall that her answer was that given the timing, things had sort of moved on, and it was the second generation laws in B.C. and Alberta that the committee should perhaps look to for direction.

Mr. Sukh Dhaliwal: Because you're collecting information from the physicians, what is their position on what we call border pharmaceuticals, when it comes to the colleges of pharmacists or doctors?

The Vice-Chair (Mr. David Tilson): Very briefly.

Ms. Anita Fineberg: The National Association of Pharmacy Regulatory Authorities does have a policy position, and they allow the information to be collected.

With respect to B.C., that was raised before, and its bylaw is quite old. It came into effect in 1997 and was effectively forced upon the college by the B.C. Ministry of Health against its wishes. The college board has subsequently voted to amend that bylaw, but the B. C. government has yet to approve the amendment.

The Vice-Chair (Mr. David Tilson): Thank you very much.

Mr. Wallace.

Mr. Mike Wallace (Burlington, CPC): Thank you, Mr. Chairman.

My questions are mostly for our friends from the National Association for Information Destruction. It was interesting for me, as in another lifetime I was in the information management on paper—I worked for TAB Canada. I don't know if you know TAB. We had a section that dealt with policies, and so on, on records management. I wasn't one of them, but I was familiar with it.

Did PIPEDA make a difference in terms of legislation? I know there was legislation, or at least guidelines, for a record of management information in terms of how long you hold onto something, when it should be destroyed, and so on.

Could you clarify for me two things right up front? Is your company in storage and in destruction? Did PIPEDA make a change to those other guidelines—I don't know if it was guidelines or legislation—on how long you keep records and so on?

Mr. Dave Carey: To answer your first question, there are various sizes of companies. For example, my company is in the records information management business, which is magnetic media and hard copy storage business and shredding. But the majority of our members are independent, shred-only, destruction-only companies.

Do you want to answer number two, Bob?

● (1000)

Mr. Robert Johnson: Number two, did PIPEDA make a difference in the behaviour of organizations with regard to disposal? Is that it?

Mr. Mike Wallace: That's part of the question. The other part of that question was, are there not already laws in other areas about—? We used to advise people that, if the information was to be kept for five years, after five years get rid of the damned stuff so you don't have it sitting around—or if it was seven, or nine, whatever the timeframe was. Has that changed?

Mr. Robert Johnson: Obviously there are still legal retention requirements. Of course you want to keep it around for its useful life as well, if there's some access to it. Certainly it is prudent records management policy, and continues to be prudent, to purge records that are no longer needed, that have reached the end of their retention period, and to do that on a regular basis to avoid the appearance of suspicious destruction. If it happens there's a lawsuit a week later, and you did it offhand, it's going to be adversely interpreted. There are all of those things. But there is no requirement to get rid of them at that period of time, and there never has been. With regard to their disposal, there's very little direction at this point other than just—

Mr. Mike Wallace: So it's guidelines, basically. Okay.

It has been referenced that Alberta and British Columbia have privacy pieces. Do they have destruction requirements in their laws?

Mr. Robert Johnson: Alberta's Personal Information Protection Act is a bit clearer than PIPEDA is, but not much. Across the board, even going back to 1990 with the Freedom of Information and Protection of Privacy Act, when it was passed at that time, it had a clearer definition or direction as far as what destruction is and that personal information shall be destroyed when it is discarded, but no definitions of what destruction is, and destruction could be interpreted as many things.

Mr. Mike Wallace: Has your organization taken the time—I know your partners at the table here today have taken stuff from another piece of legislation in British Columbia and want to put work product stuff in the federal one. Do you have the actual wording of what you would like to see?

Mr. Robert Johnson: We have supplied such wording in both the United States and in the European Union when we were asked for it. We have not prepared that for Canada at this point, but it would be very easy to do.

Mr. Mike Wallace: Okay.

The Vice-Chair (Mr. David Tilson): Excuse me, that would be useful if you sent it to the clerk.

Mr. Robert Johnson: Consider it done.

The Vice-Chair (Mr. David Tilson): Thank you.

Mr. Mike Wallace: I was interested in your question on notification. Maybe not all your members are, but some of your bigger members are in the storage business also, which means you actually have records of people, some of it very private, for storage. You are telling me now that none of these breaches that you mentioned earlier happened from a storage company?

Mr. Robert Johnson: We're not saying that. There have been incidents. We are asking for some consideration and credibility here, because we are representing our interests to some extent in being here, asking for this. I can't believe it's too often that an industry comes to you asking for more regulation that is actually going to affect it, and it will affect our members. But we have had members who store records that have had breaches and would be covered and even penalized under more stringent legislation.

Mr. Mike Wallace: That's my question.

The Vice-Chair (Mr. David Tilson): Thank you, Mr. Wallace.

Madame Lavallée.

[*Translation*]

Mrs. Carole Lavallée (Saint-Bruno—Saint-Hubert, BQ): I would like to thank you for appearing here this morning and I apologize for being late, that was unintentional.

I have a question for IMS representatives regarding work product.

In your presentation, I believe it was Ms. Fineberg who mentioned that you had supplied the committee with a number of terms for such an amendment. I have just received a copy of your brief and was unable to find those definitions.

Mr. Gary Fabian: In the English version, they are on page 34, I believe. In the French version, you can find them on page 42.

● (1005)

Mrs. Carole Lavallée: Your recommendation reads as follows:

> IMS's recommendation for a technical amendment to PIPEDA consists of two parts:
>
> (1) THAT the definition of "personal information" as found in section 2 paragraph 1 of the act be amended to read as follows:
>
> > "personal information" means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization, or work- product information.
>
> AND
>
> (2) THAT a definition of "work-product information" to read as follows be added to section 2(1):
>
> > "work-product information" means information prepared, compiled or disclosed by an individual or group as part of the individual or group's responsibilities related to their profession, employment or business. It does not include:
> >
> > (i) personal information about an identifiable individual who did not prepare, compile or disclose the information; or
> >
> > (ii) information collected, used or disclosed for the purposes of workplace surveillance.

Those are your two suggestions. Is that correct?

Mr. Gary Fabian: Yes.

Mrs. Carole Lavallée: Which one do you give greater importance to?

[*English*]

Ms. Anita Fineberg: It is not a choice with respect to the way in which we are proposing an amendment. The two parts must work together. The first part is that the definition of personal information, as it is in PIPEDA right now, would have another exclusion, which is for work product information. Then in order to accomplish that, there must be another amendment to the act, a definition of what work product information is. That is what you see in the second part.

In the work product definition itself, you have the opening phrase, and then you have: "It does not include—personal information about an identifiable individual who did not prepare, compile or disclose the information"—that is adapted from the B.C. one—"or information collected, used or disclosed for the purposes of workplace surveillance." We proposed that in the amendment to address the concerns that were expressed by a couple of witnesses who appeared before you, in particular, the federal commissioner.

[*Translation*]

Mrs. Carole Lavallée: I have a naive question for you. Who could oppose such a definition and why?

[*English*]

The Vice-Chair (Mr. David Tilson): Madam Lavallée is never naive, I might add.

Some hon. members: Oh, oh!

[*Translation*]

Mr. Gary Fabian: In my view, people might believe that their personal information could be compromised. There might be—and these are things that have occurred in the past—patients who believe that, because we gather prescription information it could be compromised, but that is not the case.

It is therefore possible that some patients see things that way. But otherwise...

Mrs. Carole Lavallée: And physicians?

Mr. Gary Fabian: Physicians could as well.

Mrs. Carole Lavallée: Are physicians opposed to such a definition?

Mr. Gary Fabian: Specifically speaking about Canada or given sectors, I'd say that some physicians are not necessarily pleased about the fact that we gather that information.

Mrs. Carole Lavallée: How come?

Dr. Léo-Paul Landry: It is quite simple to answer that, Mr. Chair. Based on our experience, physicians who are opposed do not know the company and its products. We have had the opportunity to sit down with physicians who had questions or who had research needs. From the moment they understood what it was we did, they were in complete agreement. Besides, that is the trend at present, and more and more physicians want to have their personal profiles.

[*English*]

The Vice-Chair (Mr. David Tilson): *Merci.*

Mr. Van Kesteren.

Mr. Dave Van Kesteren (Chatham-Kent—Essex, CPC): Thank you, Mr. Chairman, and thank you to the witnesses for coming.

Just for clarification, we've heard an awful lot of witnesses, and basically the only thing you're suggesting is an amendment between private information and product information. So you're quite satisfied with the act as it stands. You'd just like to see a little clarification in that area.

● (1010)

Ms. Anita Fineberg: Our position is that generally PIPEDA is working well as far as it impacts our company, but on this particular issue, on this point, we believe PIPEDA does require some clarification.

Mr. Dave Van Kesteren: We've heard a tremendous amount of information and such, and aside from all the Chicken Little evidence, I think I can narrow it down to this. At least, that's what I'm finding.

The only other thing I find interesting, gentlemen, is your presentation—A simple law applied to the act, stating that all information is to be stored, and if it's moved, it should then be moved in a certain way or shredded—could something like that just be added to the act?

Mr. Dave Carey: I'll start, and then perhaps you'll want to add to it.

What we're looking for is a formal definition on how to get rid of something at the end of its life. When the life is over, get rid of it. We're finding that "get rid of it" is too open; we're looking for a definition that says, let's obliterate it, shred it, or whatever, just a better definition.

Mr. Robert Johnson: I would just say that unless you spend as much time obsessing on this issue as we do, being in the industry—The word "destruction" means destruction. It's reasonable to think that "destruction" means something, but it still has some interpretation, and that's why we're asking that the definition of what you mean by destruction be included and explained to the readers.

Mr. Dave Carey: That's right.

Mr. Dave Van Kesteren: Have you thought about that? Have you formulated a possibility as to what that act might say?

Mr. Dave Carey: Yes.

Mr. Robert Johnson: We've included a definition, but we're going to go further and provide language that we provide to other bodies like this.

Mr. Dave Van Kesteren: You'll provide that to the committee.

Mr. Robert Johnson: We will.

Mr. Dave Van Kesteren: That's all I need to know.

Thank you.

The Vice-Chair (Mr. David Tilson): Deleting doesn't mean it's gone, I guess, does it? No.

Mr. Martin.

Mr. Pat Martin: Thank you, Chair.

Most of our witnesses in this have come with specific details that affect their particular businesses. But I'm interested as well, because you're experts in the privacy field, in a more general concern that doesn't come up as often.

When the Public Safety Act was introduced, Bill C-7, it amended PIPEDA dramatically in 2004. It allows that private sector organizations can act as agents of the state to collect personal information, without consent, for the sole purpose of disclosing this to the government.

Under these amendments, CSIS or the RCMP could now ask a business to collect new data that these agencies might otherwise not be able to collect, and they might be able to use their power under PIPEDA to conduct searches at the request of these agencies that would otherwise violate the Charter of Rights and Freedoms. Is that a concern that you have heard raised as experts in the privacy field? I know it may not pertain to your particular businesses.

This is for either or both of you. We have only a few minutes.

Ms. Fineberg.

Ms. Anita Fineberg: I've heard the concern raised, but I defer to other experts who have appeared before the committee with respect to the details.

Mr. Pat Martin: This is of great concern to the general public. Certainly the Winners-TJX-CIBC case is the one in the papers that everybody is concerned about, their personal identify theft. But I would argue that we've really gone somewhere we've never gone before with our version of the Patriot Act, almost, in terms of scope and ability. Your company might be deputized to search those records that you're storing, on behalf of the RCMP, to find my name and give it over to them.

Is this something you've contemplated within your company?

Mr. Robert Johnson: I would respectfully defer again. I have a reaction as a citizen. I'm here on behalf of the information destruction industry in that regard, so I would say as long as they properly destroy it at the end of its life, we're very happy, but—

Mr. Pat Martin: We're back to the shredding.

I think it's a great concern. Again, it's not something you came here to talk about, but the general public should be at least aware, if not very concerned. This Public Safety Act passed without a great deal of fanfare. I remember when it came through the House of Commons, we all objected to Bill C-36, the Anti-terrorist Act, for its broad sweeping powers, but this committee didn't exist then, in 2004. This is the most recent standing committee of the House of Commons. It wasn't created then, so I'm not sure the bill got the analysis that it possibly could have as it pertains to PIPEDA.

I guess I don't have a great deal to add to that. If I have any time left. that's the only thing I would like your comment on, but both of you have chosen not to, so—

● (1015)

Mr. Dave Carey: As a personal citizen, as an individual Canadian, I would be concerned, and I believe my company, which is in the records management business, would have problems being deputized, as you say, to start going through records and finding information on behalf of—I think it would be very difficult.

Mr. Pat Martin: Who do you think your loyalty would lean towards? I mean, you have an obligation and a contractual promise to the people whose records you're keeping to keep them private, but now the RCMP or CSIS could say you have a second obligation to them not to keep it private, but to blurt it out.

Mr. Dave Carey: Absolutely. Our contracts physically state that the privacy factor and the confidentiality of our customers as a whole are very important, but obviously the law—

Mr. Pat Martin: You might not be able to make that commitment anymore—

Mr. Dave Carey: Absolutely.

Mr. Pat Martin: —subject to this Bill C-7.

Mr. Dave Carey: Possibly, yes.

Mr. Pat Martin: That's scary isn't it?

The Vice-Chair (Mr. David Tilson): Mr. Peterson.

Hon. Jim Peterson (Willowdale, Lib.): Dr. Rosenberg testified that in many cases it's fairly simple to re-identify patients. How does IMS make sure this can't be done?

Ms. Anita Fineberg: There are a number of ways to ensure that it can't be done. At first instance, the information that we receive from our data suppliers goes through a software program that leaves anything related to the patient behind. So that's at first instance, and then we have technological means to ensure that everything is totally screened out. As well, all of our contractual provisions prohibit any provision of anything that might identify a patient to us.

As I mentioned before, we are a strong supporter of patient privacy rights with respect to personal health information, and collecting anything that might identify a patient is illegal in this country, not only under PIPEDA but under all the privacy legislation. We would expect any organization that might engage in that kind of activity to be called to account and that the legislation would be enforced against them.

Hon. Jim Peterson: Who could possibly object to what you're asking for?

Ms. Anita Fineberg: I agree, and I was considering Madame Lavallée's question, and I appreciate your asking it again. The short answer is, subject to what Dr. Landry said, nobody that I know of, quite honestly. And I think you've heard from a wide variety of representative organizations and groups who have appeared before the committee, all of which support the distinction. I think one thing —

Hon. Jim Peterson: My only problem is this. I don't know whether the amendment you've suggested is the proper way to do it. I'd be happy to propose an amendment saying IMS is not in breach. But, for example, the amendment you've proposed is quite different from what B.C. has put in.

Ms. Anita Fineberg: No, it's not.

Hon. Jim Peterson: Well, it's different. It's worded differently.

Ms. Anita Fineberg: It has the added part in part 2, the little exclusion, to make sure to address the commissioner's concern that workplace surveillance information might not be inadvertently captured. I think, given that you've heard from different groups, there's a wide spectrum of work product information out there that is of concern to different organizations.

We have a particular concern with respect to the prescription information, but any memorandum, any letter, any opinion, any document created by employees or professionals as part of their business responsibilities, if we do not proceed with this work product exclusion, could well be considered to be personal information.

I know that the commissioner in B.C. addressed the access issue, and the committee has spoken about small business concerns with respect to compliance. Ex-employees could say that anything they wrote or put their names on when they worked for you is their personal information. They could leave, put in an access request for all of that, every e-mail. From a business perspective, particularly smaller business perspective, they could get totally snowed under.

● (1020)

Hon. Jim Peterson: I wouldn't mind hearing, Mr. Chair, from anybody—maybe previous witnesses—who has concerns with the precise wording of the amendment that's been suggested.

The Vice-Chair (Mr. David Tilson): The commissioner's coming. She may have some thoughts.

Hon. Jim Peterson: That's a good idea, yes, thank you.

The Vice-Chair (Mr. David Tilson): Are you finished, Mr. Peterson?

Hon. Jim Peterson: Is there an association that protects the other side of your enterprise—for dumpster divers or things like that?

Mr. Dave Carey: I would not think so.

Mr. Robert Johnson: I don't think they've unified yet, although I do have an article here on a theft ring that specialized in dumpster diving to get private information and capitalize on it.

Hon. Jim Peterson: Is it fairly widespread?

Mr. Robert Johnson: Very much so. It's the primary source of the information that goes into identity theft. It's hard-copy access. These are not high-tech breaches.

The Vice-Chair (Mr. David Tilson): Dumpster diver—that's one of the main things the committee's learned in this session.

Go ahead, Mr. Wallace.

Mr. Mike Wallace: Thank you, Mr. Chair.

I just have a really quick follow-up, because I was politely cut off.

I wanted to ask the information management folks about the question of notification. I was interested to hear you say that you want to extend that or have more detailed notification requirements. The commissioner has come to tell us previously—and we're going to have the commissioner back—that the notification system we have now is adequate and that, if possible, notification is not required and the issue gets resolved internally. Then nobody's hurt by it and that's sufficient.

Have you actually surveyed your members so they know that they will be more liable, based on your presentation today, if there is a change to the notification piece, in that, as some have argued, for any breach at all there should be notification to the person?

In my mind, a lot of records in this country are stored near warehouses, and sometimes they get destroyed and sometimes they don't. I think you're at a higher risk than many. So I'd like to know for sure that I can say that I heard from your organization, and that you have surveyed your members, and they are confident that you are right that there should be a greater notification process than what exists now in PIPEDA.

Mr. Robert Johnson: I think one of the reasons that NAID Canada and NAID Europe have been such a most credible source, of information is that we don't always take a position that might be the best economic thing for our members. We actually use this as a consumer advocacy organization, by our mission and charter.

We're supported by the industry. We took a position on professional liability insurance requirements for our members that cost them a lot of money, and I got a lot of hate mail as a result, but that was the right thing to do. In this case, we feel that notification is the right thing to do. Our members support NAID having an entree to venues like this because of that credibility, and they continue to support the association, even if we might take a position in that way.

That said, I think that if we were to in fact go to members and ask them—and we have not taken that survey—they would definitely see the benefits to the consumer, as well as the benefit to the industry, to have notification provisions that not only extend to high-tech, sensational electronic breaches, but include in that notification people put at risk by the casual disposal of hard-copy documents.

Mr. Mike Wallace: Let's say somebody breaks into a warehouse, steals some boxes, and the stuff ends up on the streets of Toronto. If they found out it came from Iron Mountain, it could hurt the business considerably. Are you telling me, today, that you are willing to take that risk?

● (1025)

Mr. Dave Carey: In our particular case, yes, absolutely. We have an internal notification policy in place for situations exactly like that. Even without your legislation, as a records management company we have an internal policy of notification.

Mr. Mike Wallace: Thank you very much.

Thank you, Mr. Chairman.

The Vice-Chair (Mr. David Tilson): That concludes the second round.

We have three more individuals who wish to ask questions.

I have one brief question to Ms. Fineberg.

I represent a community that has a lot of little villages and towns. Everybody knows everything about everybody. It's wonderful. You indicated that the information you receive is anonymous. It may be in the big city, but it's wonderful how people find things out in these communities. You may live next to someone and your neighbour knows everything about what you're doing.

Is it possible that people could piece together the little pieces of information you have and then it's no longer anonymous?

Ms. Anita Fineberg: I come from one of those small towns too, by the way.

We have had our data examined, from a number of different perspectives, to address precisely those types of questions. We've had statisticians from McGill look at our internal databases with respect to whether you can slice and dice and potentially combine anything to identify an individual. The expert answer was no. There are contractual provisions in place with respect to our employees not being able to do anything with the data except process it internally to undertake that exercise.

The Vice-Chair (Mr. David Tilson): The problem is that people guess. They're very good at guessing. I don't want to make a big deal of it. I'm just telling you that from the community I personally represent—and there are other members of this committee who represent similar communities—people are very good at piecing these little pieces of information together. That's all I'm saying. And they challenge the experts.

Mr. Dhaliwal.

Mr. Sukh Dhaliwal: Thank you, Mr. Chair.

My question, again, will be to IMS. I will continue where Mr. Pearson left off.

When it comes to long-term planning, I can see why these definitions of work product and personal information are very important. From a business perspective, I can see where their case is covered.

I wonder how all this work that IMS does would help the consumers in a small community like Mr. Tilson's. How are you helping communities like that? Are there any benefits?

Mr. Gary Fabian: I think that's a perfect example of where the IMS data, the availability of such a comprehensive database—and those were some of the issues I cited in my opening remarks.

We've done extensive work in the research community on specific diseases such as the treatment of infection and antibiotics. There was an educational program launched in Alberta, called "Do Bugs Need Drugs?", and they needed comprehensive and authoritative information to find out if the program was actually working. We were able to provide the small community with information about whether the program was actually working and whether there was a change in the general consumption of anti-infectives. It was very simple things, such as teaching people to wash their hands, cleanliness and things like that, right up to not asking your doctor for an anti-infective every time you visit because you have a sore throat.

Without our information they weren't able to tell if people's habits were changing, whether physicians were prescribing differently, and whether people were taking fewer anti-infectives. That's a very good example of one that worked in a small community.

Similarly, we did extensive work for the Collège des médecins in the province of Quebec on the use of ritalin in children. They had no supporting information about that. It was a perfect example. You had educational and health issues, with children, physicians, and parents involved. They needed strong empirical evidence, and we were able to provide it.

Without the kind of basic information we collect, you wouldn't be able to provide that. Nobody else has it. The governments don't have it and no other research organization has it.

● (1030)

Mr. Sukh Dhaliwal: That answers my question, Mr. Tilson. Thank you.

The Vice-Chair (Mr. David Tilson): Thank you.

Madam Lavallée.

[*Translation*]

Mrs. Carole Lavallée: Let me come back to your definition of work products. And I quote: "[...] information prepared or collected by an individual or group of individuals as a part of the... responsibilities [...]"

I will omit reading it out. I have a question for Mr. Carey of the National Association for Information Destruction - Canada.

Does this definition cover the kind of work products that you have? When you receive documents for shredding or destroying by some method, can you say that you are receiving work products?

[*English*]

Mr. Robert Johnson: Our members provide service in a relatively amoral and antiseptic environment. We are contracted to destroy media containing information. We have no concern about what is on that medium other than that the client who hired the member wants it to be properly destroyed. So we really don't know whether it's competitive information they want to have destroyed, personal information about their customers, or it's just the way they've chosen to get rid of all of their media so that no one ever sees it when its destroyed, and they know its fate. The meta-information that may be on that, or what the information is, is really of no issue to us once we've been contracted to destroy it.

[*Translation*]

Mrs. Carole Lavallée: Nevertheless, the documents that you receive do contain information prepared or collected by an individual or group as a part of the responsibilities related to their employment or business. Am I right?

[*English*]

Mr. Robert Johnson: Yes.

[*Translation*]

Mrs. Carole Lavallée: Therefore, this is the definition of work products that you have adopted, is it not?

[*English*]

Mr. Robert Johnson: Quite respectfully, I do not think the distinction between private information, personal information, or work product is applicable to our situation, because we provide those services that we provide only because the client asked us to do it. In a perfect environment, which we try to create, our employees never see the information and don't know what it is. So for us it's in some respects all work product, because we have no regard at all for what is on the materials. We handle it all very securely because that's what the client wants us to do. We have no idea what really is on the medium or where it comes from.

Mr. Dave Carey: We would also destroy material that's not under that definition.

Mr. Robert Johnson: Maybe the better way to look at it is that we consider everything we take, because that's our charter, as highly confidential and private, of the utmost privacy. It may not be. It may be work product that is totally stripped of all identifying information about individuals. That is not our decision to make. We were hired to treat it as confidentially as possible, and that's what we do.

[*Translation*]

Mrs. Carole Lavallée: My question is for the representatives of IMS Health Canada.

You often use prescriptions as an example. To begin with, does every pharmacist agree to give you information on prescriptions? Are there any who refuse? Do they have the right to refuse?

Mr. Gary Fabian: They have the right to refuse.

Our work consists of sampling. There are more than 7,500 pharmacies in Canada. We cannot gather information from all of them because it is not necessary and because we could not afford it. Our company's work consists in making projections in view of universal levels.

In answer to your specific question, pharmacists are under no obligation to provide us with information if they do not wish to do so.

Mrs. Carole Lavallée: You gather information from health professionals, like pharmacists.

Mr. Gary Fabian: Yes.

Mrs. Carole Lavallée: From physicians?

Mr. Gary Fabian: Yes.

Mrs. Carole Lavallée: And how about dentists?

Mr. Gary Fabian: If a dentist prescribes a drug.

Mrs. Carole Lavallée: Are drugs your main focus?

Mr. Gary Fabian: Basically, they are.

Mrs. Carole Lavallée: If I understand correctly, the people who object to your definition are health professionals who might be identified through your work. Could they be identified?

● (1035)

Mr. Gary Fabian: Do you mean health professionals such as physicians?

Mrs. Carole Lavallée: Let us say that you might notice that a physician is prescribing Valium to all his patients.

Mr. Gary Fabian: Once again, as Ms. Fineberg explained at the outset, this is the very aspect we want to protect, up to a certain point. The information that we provide is always part of a vast aggregate of data. A minimum of 30 physicians is always required to make up a group, but there could be as many as 150 or 1,000.

Therefore, it is really impossible to single out a physician and to say that he was the one who prescribed such and such a drug. The physician is included in a group that prescribes certain kinds of drugs. Our objective ends there. That is as precise as we get.

Mrs. Carole Lavallée: All right, you cannot do that.

[*English*]

The Vice-Chair (Mr. David Tilson): *Merci*.

It came up in one of our hearings, through one of our guests who came, that the B.C. pharmacists had passed a resolution that they would not release information.

Ms. Fineberg, do you know about that, and do you have any comment about it?

Ms. Anita Fineberg: Certainly. It's actually a reference to a bylaw that was passed by the B.C. College of Pharmacists in 1997. Effectively, the college was mandated by the B.C. health minister at that time to change its bylaws to effectively prohibit the disclosure of any information that identifies a physician for the disclosure for commercial purposes.

Since 1997, the board of the College of Pharmacists has voted, I believe it's three times now, to amend that bylaw to remove that prohibition, but because the approved bylaw must be approved by the B.C. government through an order in council, that has yet to be done.

The Vice-Chair (Mr. David Tilson): So in British Columbia that's the law?

Ms. Anita Fineberg: The situation is that you have that bylaw, and as you've heard, you have the B.C. PIPA, which excludes work product, which would exclude the type of information. From a legal perspective, there are opinions out there that because one is a law—i.e., PIPA's a law—and the other is only a college bylaw, legally the PIPA exclusion would take precedence over the college bylaw. But there are also practical realities of doing business.

The Vice-Chair (Mr. David Tilson): Mr. Martin.

Mr. Pat Martin: Thank you.

There's another piece of legislation that's going through the House of Commons right now that has an implication I'd like your views on. They want to change the permanent voters list for identification to try to deter voter fraud. And I should tell you there was one case of voter fraud in the last federal election, none in the election before, and three in the election before that. But the permanent voters list would now have your name, address, telephone number, and date of birth.

I had something like 200 volunteers in my election campaign, and it's not unusual to tear off a sheet of the voters list and give it to one of your volunteers and say, canvass these 50 people. As privacy experts, do you have any comment on that? Dumpster divers love to find date of birth. It's like a PIN number.

Mr. Robert Johnson: Yes. My comment would only be that when we look at proposed regulations regarding information protection, very often we do recommend that the definition of personal information be expanded.

We mentioned the Georgia state shredding law, which we like to use as an example. That law excluded phone numbers as a piece of personal information, much as PIPEDA does. We disagree with that as an association because, as always, it's the ability to coordinate several pieces of information that give you the critical mass—

Mr. Pat Martin: You can get that from your phone book, though. Name, address, and phone number is pretty accessible.

Mr. Robert Johnson: I understand, but if it's matched with an account number and matched with an address and with the name, it becomes kind of a ballet for those experts: how many different pieces do they have to be able to put your mosaic together?

Mr. Pat Martin: What if you add date of birth in there?

Mr. Robert Johnson: That is my point. The things you exclude are the things that they're going to put together to make the mosaic.

Mr. Pat Martin: So if the government does it for you on the permanent voters list, isn't that a recipe for identity theft?

Mr. Robert Johnson: I won't go so far as to say that. It certainly could aid and abet those trying to do that.

● (1040)

Mr. Pat Martin: Do you have any opinion on that, Ms. Fineberg?

Ms. Anita Fineberg: Only to suggest that perhaps the way to address the issue is to tightly control what happens to that extra piece of information, the date of birth, once it's used for the alleged purpose that it's necessary for—i.e. to confirm the identity of the voter to prevent fraud—and then it disappears after that from any subsequent circulation or documentation.

Mr. Pat Martin: That's interesting.

My other questions brings us back to the—You want to destroy everything.

Some hon. members: Oh, oh!

Ms. Anita Fineberg: That's right—[*Inaudible—Editor*].

Mr. Pat Martin: Coming back to the B.C. privacy commissioner's testimony, he raised the issue that in the sale or transfer of a business, sometimes the database or the customer list is the most valuable part of that business. He was saying that in B.C. this is guarded, and I guess the obligation of privacy is passed along to the successor company.

But do you think PIPEDA should be amended in a similar way? Also do you think that individuals should have the opportunity to opt out of being on that list; in other words, should they be notified?

For instance, regarding the census, I don't want Lockheed Martin having my personal information. In fact, there was a whole boycott being planned in Canada that, if Lockheed Martin gets the census, we're not going to cooperate with it. Do you think people should have the opportunity to opt out of being on a list if the business sells, and should PIPEDA address this?

Mr. Robert Johnson: Personally I would like more time to think about that before I declare myself. Certainly I could see how someone would be concerned, and it seems to me a reasonable proposition that because I've entrusted my information to one entity, if they sell their business or do business with another entity, I should be aware of that.

At minimum, our recommendation said that there should be a very clear contract that specifies the fiduciary responsibility, the chain of custody, and the obligations under whatever regulations exist within the jurisdiction to which the information was originally entrusted to the first custodian.

Mr. Pat Martin: That might help from a legal point of view, but what if I'm openly hostile to a company? What if I don't just dislike the company that's being sold or is buying my information, but I don't want anything to do with them? Do I not have a right to withdraw the information that I confided into company A, which I don't want to be controlled by company B? Where are my rights there?

Mr. Robert Johnson: There's the practical—and then I think the presupposition of all privacy legislation as a human rights issue is that it's actually the person the information is about who should be the ultimate decision-maker on where that information can go. If that's where the basis of it all starts, I think that might answer your question.

The Vice-Chair (Mr. David Tilson): Thank you, Mr. Martin.

Does Ms. Fineberg have an opinion on this?

Mr. Pat Martin: I don't know. You could ask her. But these questions should go to other witnesses, if they want to comment.

Ms. Anita Fineberg: The only comment I would make is that I believe some of the witnesses, including the B.C. privacy commissioner, were dealing with the particular issue in the context of what an organization would be able to disclose about either its clients or employees in a prospective purchase in the mergers and acquisition situation. Both the B.C. and Alberta legislation accommodated those situations, because sometimes a company cannot legally disclose to anybody, either to its employees or its clients, that there's a deal in the works, because this would be in breach of securities legislation, if it's a publicly traded company.

The Vice-Chair (Mr. David Tilson): I'll have to put you down again, Mr. Martin.

Mr. Dhaliwal.

Mr. Sukh Dhaliwal: To continue where I left off, my last question is to Mr. Fabian.

You mentioned how it will help small communities such as Mr. Tilson's and Ms. Fineberg's, and many other small communities, in research and development. When you take this prescription information, can you distinguish between what is used for business purposes and what is used for research and development?

As a follow-up question, if you don't have that information available for commercial or business purposes, what are the consequences for consumers?

● (1045)

Mr. Gary Fabian: I think the distinction between what is used for commercial purposes and what I already described is in the example of pharmaceutical companies that spend enormous amounts of money on research and development to come up with new therapeutics, and so on. They need to develop their strategies. They need to understand disease states and what's coming in the future.

We have an aging population that's very concerned about what kinds of medications they're going to need to be developed. The pharmaceutical companies need to enlist physicians for clinical trial purposes, they need to provide information for continuing medical education purposes to the physician community, and they also need to provide general information about their products specifically to the medical communities and to the pharmacy sector as well.

So I think that's the clear distinction you can make between the antibiotic usage I gave you, where you have real clinical research, and then the more commercial needs.

Ms. Anita Fineberg: If I might, I think there are a lot of areas where it's certainly impossible to draw that bright line with respect to research. Gary mentioned clinical trials and the use of the information by pharmaceutical companies to get the word out to physicians about clinical trial work. I think we'd all agree that clinical trials are health research. So where do you draw the line there? Where do you draw the line when you're talking about providing information and education about particular products and services to the health profession groups?

So I think it's difficult in many cases to distinguish between purely commercial purposes and research purposes. And the other thing we have to remember, of course, is that in Canada these days much of the health research that's conducted, on pharmaceuticals in particular, is conducted by the private sector.

Mr. Sukh Dhaliwal: You have both spoken.

What about Dr. Landry? What is his perspective, and as a doctor, what does he see the consequences being if that work product definition is not clearly defined in the act—from a consumer perspective?

Dr. Léo-Paul Landry: Let me put it this way. The concept of work product as opposed to the concept of privacy and personal information represents two different interests. The work product serves to inform the provider side of a provider-consumer relationship, in our case physician-patient. So the work product serves as a tool that informs the provider in that relationship, with the object of providing better services.

We're in a situation right now in this country where leaders in continuing medical education are discovering progressively the value of the information we can provide. Some of them want to use, or some of them are using, these tools to help physicians identify their own needs in terms of continuing medical education. Those who realize the value of this product would be at a loss if we were not able to continue this. As we meet more and more physicians and explain what we have and what we can provide as a service, the eyes all of a sudden open up and they say, “There's value to that”. As a matter of fact, it goes beyond what they ever imagined.

I hope I'm addressing your question.

Mr. Sukh Dhaliwal: Thank you, Mr. Chair.

The Vice-Chair (Mr. David Tilson): We're coming to the conclusion, and I have a question to our IMS guests.

I'd like to read a quotation from the *Business Law Journal*, October 2006, from an article written by Lisa M. Austin. I don't know whether you're familiar with this. It gives the other side of the coin in terms of what your position is. I'd like to read it to you and ask for your comments.

This is on page 31 and page 32:

> And despite the Privacy Commissioner's assertion that prescription information provides little information about the physician, it is important to understand that pharmaceutical companies seek this information in part because they think that it does. They use this information to compile personalized physician prescribing patterns that they can then use for purposes of targeted marketing—a practice that many physicians object to if it is done without their knowledge or consent.

That gives the other side of what you're saying, and I'd like you to comment on that.

● (1050)

Ms. Anita Fineberg: Sure. Perhaps Dr. Landry, as a physician, might answer.

Dr. Léo-Paul Landry: I'm just trying to figure out how to respond to that.

That's not reality in Quebec. First of all, the whole medical profession in Quebec knows exactly what we do. As Anita has alluded to, it's on our website. They get the IMS journal. We go to great lengths to provide all the information, so it is done with their knowledge across the province. That's number one.

Number two, I can understand that some might not like that, but on the other hand, a lot of physicians don't like to be approached by a whole variety of pharmaceutical reps in areas of no concern to them. More and more physicians are focusing on an area of practice and they want to deal with pharmaceutical companies that have products for their areas of interest. So part of what we do helps the pharmaceutical industry target physicians who are really using or prescribing their medications.

On the other hand, it prevents them from approaching physicians who have no interest in these, so there's a benefit to that. As a matter of fact, there is significant benefit to that, because in cases that I know of personally, physicians have a relationship with the pharmaceutical reps and get scientific information from them, especially in relation to side effects. And that's a reality.

As a matter of fact, two weeks ago I was in the hospital milieu and I heard about these things, and then we saw reps. The whole approach of pharmaceutical reps has changed over the years and it's become much more scientific, so there's value there. And that's the counter, the other side of the coin that you present.

The Vice-Chair (Mr. David Tilson): I want to thank both groups for coming and giving us your views. You've stimulated some conversation for us, and I appreciated your doing that. So thank you very much for coming.

Before we adjourn, members of the committee, our chairman, Mr. Wappell, will be returning next week. We're approaching the end of this review, and I believe that somewhere along the line we're going to be asking for the report to be prepared. Normally the Library people, Ms. Holmes or whoever, prepare a summary of the recommendations that have been made by witnesses, the proposed amendments. And the question I have is, do we wait until the end when we've heard from the minister—and I think the minister is coming, and the commissioner—or do we have a draft report before they come, so they can hear the proposed amendments from our witnesses, and ask them to comment on that when they come.

I'm not asking for an answer now. This is something that perhaps the chair should deal with when he returns, but it's an observation I have made in my position today, that we should be thinking ahead as to how we're going to prepare our report. So I'll leave that with you.

Again, thank you for coming.

The meeting is now adjourned.

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

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

Also available on the Parliament of Canada Web Site at the following address:
Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante :
http://www.parl.gc.ca
