HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Industry, Science and Technology

INDU • NUMBER 038 • 2nd SESSION • 41st PARLIAMENT

EVIDENCE

Tuesday, March 24, 2015

Chair

Mr. David Sweet

Standing Committee on Industry, Science and Technology

Tuesday, March 24, 2015

● (1105)

[*English*]

The Chair (Mr. David Sweet (Ancaster—Dundas—Flamborough—Westdale, CPC)): Good morning, ladies and gentlemen. *Bonjour à tous*.

Welcome to the 38th meeting of the Standing Committee on Industry, Science and Technology.

Thank you to the witnesses for coming today. I will introduce them: from the Public Guardian and Trustee of British Columbia, Catherine Romanko, public guardian and trustee; from the Public Guardian and Trustee of Manitoba, Douglas Brown; from the Canadian Pharmacists Association, Janet Cooper, vice-president, professional affairs; and as an individual, Avner Levin, associate professor and the director of the Privacy and Cyber Crime Institute at Ryerson University.

We will follow that order as far as opening remarks are concerned.

I just want to advise members that we have another committee coming in here after us, so we'll be targeting for five minutes before our usual time to complete.

We'll begin with opening remarks from Ms. Romanko.

Ms. Catherine Romanko (Public Guardian and Trustee, Public Guardian and Trustee of British Columbia): Thank you, Mr. Chair.

Good morning. I am the public guardian and trustee of British Columbia. I thank you for the opportunity to comment on Bill S-4 today. In addition to my oral comments, I have provided a written submission. My comments today are restricted to subclause 6(10) of Bill S-4, and that is with respect to the proposed provision that will enable federally regulated organizations and in particular financial institutions to report concerns of potential financial abuse of a customer, without the knowledge or consent of the customer, to a government institution with authority to investigate and to take appropriate responsive action.

The jurisdiction to respond to suspected financial abuse typically falls to provincial authorities and territorial authorities with respect to civil investigation and in particular to public guardians and trustees across the country. The Public Guardian and Trustee of British Columbia has participated in the multi-year consultation process that led to the development of the anti-financial abuse provisions in subclause 6(10). My office supports the objective of the proposed anti-financial abuse amendment and offers three recommendations for refinement of the provision to ensure that the provision is effective, and secondly, to minimize the risk of harm to an individual who is the subject of a report and a potential victim of financial abuse.

My recommendations are based on the experience my office has in responding to financial abuse and I will provide those recommendations at the conclusion of my comments.

By way of background, the Public Guardian and Trustee of British Columbia is a statutory corporation sole created under the laws of the province. My office provides fiduciary and protective services to vulnerable adults, to persons who are mentally incapable, to minor children. We administer the estates of deceased and missing persons when there is no one else able and suitable to do that. We serve approximately 29,000 clients and administer almost $900 million in private client assets.

Among the various statutory functions given to the Public Guardian and Trustee under British Columbian law is the role of investigating allegations of financial abuse, including financial neglect and financial self-neglect of mentally incapable adults. The definitions of financial abuse, financial neglect, and financial self-neglect, which guide the investigations of the Public Guardian in British Columbia, are set out in legislation, but generally speaking, abuse is an action committed by a third party. Neglect is the failure of a third party to act, and self-neglect is an individual's own failure to manage his or her own affairs due usually to mental incapacity.

When my office receives information that an adult may be mentally incapable and may be a victim of financial abuse, the Public Guardian and Trustee of British Columbia has a legislative mandate to investigate the circumstances. My office has the powers to seek disclosure of financial information from legal representatives such as an attorney acting under an enduring power of attorney, and from financial institutions where an adult may hold assets. If my office has reason to believe that the adult's assets are in need of immediate protection, the Public Guardian and Trustee of British Columbia has the authority to instruct financial institutions to, in essence, freeze bank accounts to stop any withdrawals from the accounts or transactions with respect to those accounts, to halt the sale of property, and to take any other reasonable step necessary to protect the adult's assets from dissipation or misappropriation.

Each year, my office responds to approximately 1,600 allegations of suspected financial abuse. Approximately 1,200 of those cases result in a full investigation by my office, and of approximately 400 cases, the Public Guardian and Trustee is appointed committee of estate as a result of the investigation, and that is for the purpose of acting as property guardian to manage the financial and legal affairs of the adult on an ongoing basis.

The experience of my staff in responding to allegations of financial abuse has highlighted for us the critical role played by financial institutions in identifying issues of potential financial abuse and ensuring that vulnerable adults receive the support and assistance they need when it is required in order to curtail or end the financial abuse.

● (1110)

Employees of banks are often in the best position to observe potential financial abuse as a result of ongoing personal contact with their customers and with their knowledge of the customers' financial affairs. While it may be best practice for a bank employee to communicate with a customer directly about concerns of potential abuse, in many cases such communication is simply not practical, nor is it prudent. In some instances, bank customers may have diminished mental capacity due to mental illness or due to diseases of aging, making direct communication with a customer challenging and often ineffective.

In other cases, a customer may be unduly influenced by or subject to the control of another person, so that advising the customer of suspected financial abuse may in fact alert the abuser to the fact that the abuse has been discovered and put the customer at greater risk. Currently, PIPEDA permits financial institutions to report financial abuse to relevant authorities, such as the police, where the financial institution has reasonable grounds to believe that a law has been contravened.

However, if no law is contravened, federally regulated organizations are restricted by the act as to what actions they are permitted to take even if financial abuse is suspected, so my office of course is responding to allegations of abuse, not certainties. No crime has been committed as yet. Enabling financial institutions to proactively report concerns of potential financial abuse to an organization such as the Public Guardian and Trustee of British Columbia, with the legislative authority to investigate and to take steps to protect the assets of the vulnerable adult if necessary, is critical in the effort to reduce the incidents or continuation of financial abuse.

The Public Guardian and Trustee of British Columbia offers three recommendations for refinement of the proposed legislative amendment in proposed paragraph 7(3)(d.3) of PIPEDA. They are as follows.

One, specify that provincial authorities, and in particular public guardians and trustees, who are authorized to respond to financial abuse, are included in the term “government institution” to which an organization may report financial abuse. The term “government institution” is currently not defined in PIPEDA, nor is a definition proposed in Bill S-4.

The difficulty here is that the act is a federal legislation governing federally regulated bodies. Public guardians and trustees fall under provincial jurisdiction. We want to ensure the legislation is clear that reports may be made to provincial bodies. The act contains regulation-making power, which would permit the creation of a regulation to define “government institution”.

Making it clear that organizations are authorized to report to provincial and territorial government institutions, and in particular public guardians and trustees across the country, will assist financial institutions in effectively reporting. Another alternative, of course, would be simply to provide the definition directly in the act. Either way, the definition would be very useful.

Two, delete the reference to “next of kin” from the list of individuals and government institutions to which organizations may report concerns of potential financial abuse. The perpetrators of financial abuse, particularly with respect to vulnerable adults, are often next of kin. Disclosure of concerns of potential financial abuse to next of kin may have the effect of alerting the abuser to the fact that the abuse has been discovered and may in fact end up putting the vulnerable adult at greater risk of harm—or at least the adult's assets at greater risk of harm.

Three, explicitly recognize financial neglect and financial self-neglect in proposed provisions, along with financial abuse. Many provincial authorities have statutory power to investigate and assist individuals who are victims not only of financial abuse but of financial neglect and financial self-neglect, the effects of which can be equally devastating. In fact, the indicators of potential financial difficulty are the same, whether it's abuse, neglect, or self-neglect. Permitting financial institutions to report concerns of financial abuse, neglect, and self-neglect of their customers, I submit, would protect the interests of vulnerable British Columbians.

Those are my comments. Thank you very much. I'd be pleased to answer questions.

● (1115)

The Chair: Thank you very much.

We'll now move to Mr. Brown, please.

Mr. Douglas Brown (Public Guardian and Trustee, Public Guardian and Trustee of Manitoba): Thank you for the opportunity to comment on Bill S-4, the digital privacy act. I'm Douglas Brown, the public guardian and trustee of the Province of Manitoba.

My comments today will be limited to subclause 6(10) of the bill, which would amend the Personal Information Protection and Electronic Documents Act to permit the disclosure of personal information about an individual by an organization to a government institution in circumstances where there is a suspicion that the individual may be a victim of financial abuse. The Public Guardian and Trustee of Manitoba supports the amendment as a positive step that strikes the necessary balance between the need to maintain privacy of personal information and disclosure of that information to potentially identify and stop what are the devastating consequences of financial abuse.

The Public Guardian and Trustee of Manitoba, or PGT, is a corporation sole established under The Public Guardian and Trustee Act of Manitoba, that operates as a provincial government special operating agency. The PGT manages and protects the affairs of Manitobans who are unable to do so themselves and have no one else who is willing or able to act. This includes mentally incompetent and vulnerable adults, deceased estates, and children. The PGT manages approximately 5,800 clients, estates, and trusts, with approximately $230 million of assets under administration by our office.

The PGT becomes involved in the management of an individual's financial affairs in a variety of ways. Most frequently, the PGT is appointed by the chief provincial psychiatrist under The Mental Health Act or by an order issued under The Vulnerable Persons Living with a Mental Disability Act, both Manitoba legislation. The PGT can also be appointed by a judge of the Court of Queen's Bench of Manitoba to act in various circumstances. When the PGT does become involved, an investigation is conducted to gather and record the assets owned by the individual for whom we're now managing affairs. This includes all their property, investments, and any accounts at financial institutions. Unfortunately, in some situations our investigation will uncover evidence of possible financial abuse. In the worst of these situations, the financial abuse has resulted in all or a large part of the finances of that individual having been lost.

The impact of these losses caused by financial abuse cannot be overstated. As you or I choose to save, invest, or plan for our retirement and anticipate having the financial resources to be independent and exercise some level of control over our affairs in the future, people who have been the victim of financial abuse have lost that independence and have lost that control over their futures. Often we see that the health and well-being of the victim of financial abuse can be negatively impacted. More often than not, a victim of financial abuse has little chance of recovery. In many cases the money is gone, and there is little likelihood of recovering the money from the perpetrator of the abuse.

Organizations such as financial institutions can play an important role in detecting possible financial abuse through their ongoing contact with the public. My experience is that these institutions do want to cooperate with government institutions when they have a suspicion of financial abuse. While the privacy objectives of the existing legislation are clearly important, privacy laws should not become a tool used by perpetrators of financial abuse to avoid detection. Amendments that allow for a controlled disclosure of personal information in limited circumstances can still maintain privacy objectives while also providing an additional set of eyes out in the community to help identify and hopefully stop cases of financial abuse. I would strongly recommend to this committee that this is the right result.

In reviewing the amendments and the various submissions that have been made to the committee, there are a couple of recommendations that I would also support.

First is that the definition of "government institution" needs to be clear. The PGT or similar agencies in other provinces or territories have a role in these situations, and should be included in the definition. There should be caution taken not to apply the definition too narrowly, as this could discourage the reporting of information. A reasonable check and balance to apply could be to look at the role and use of the information that could be made by the institution that is receiving the information. In the case of the PGT, we're subject to provincial privacy laws. We also have specific statutory authority that allows us to collect information that would otherwise be private where it's required to carry out our duties, responsibilities, and powers. By having that control, you've put some control over how the information could be used once it's received by a government institution.

● (1120)

Second, in most cases the perpetrator of financial abuse has to gain the trust of the victim before the abuse can begin. This unfortunately means that relatives and family can often be the perpetrators of financial abuse. Any requirement to report suspected financial abuse in all circumstances to next of kin may place the victim at greater risk. Organizations that are contemplating making a report should have some discretion in those situations, and where appropriate, should make the report only to a government institution and not to the next of kin in circumstances where the next of kin may be involved in the abuse.

Third, in some cases an individual may not be a victim of financial abuse but is no longer capable of managing his or her affairs. The indicators of financial abuse and financial neglect can often be the same, so an organization that's contemplating whether to report should have the ability to report suspected financial abuse even though it may not be clear where the unusual financial activity originates, or whether the irregular financial activity is a result of a third party or the individual himself or herself. The organization should not be required to make this determination before it has the ability to make a report to a government institution. The loss of financial independence resulting from neglect is just as significant as a financial loss caused by a third party, so again, it's in everybody's interest that the matter be identified and dealt with as quickly as possible.

In conclusion, while the privacy objectives of the existing legislation are clearly important, the benefit of permitting disclosure of personal information in a limited and controlled manner would be a positive step in detecting and hopefully stopping cases of financial abuse.

Thank you.

The Chair: Thank you, Mr. Brown.

Now on to Ms. Cooper, please, for your opening remarks.

Ms. Janet Cooper (Vice-President, Professional Affairs, Canadian Pharmacists Association): Thank you.

Good morning. My name is Janet Cooper. I am a pharmacist and I am vice-president of professional affairs with the Canadian Pharmacists Association. I am pleased to be here today to discuss Bill S-4, an act to amend PIPEDA.

CPhA, the Canadian Pharmacists Association, is the national voice for Canada's 39,000 pharmacists. Pharmacists practise in a range of settings, including community pharmacies, hospitals, academia, industry, and government.

CPhA and the pharmacy profession have a long history of speaking out for the interests of patient privacy and confidentiality, and as far back as 2001 CPhA was involved with a privacy working group of other health care provider organizations that provided advice to Health Canada on privacy matters related specifically to health care. Since then we've appeared before parliamentary committees on numerous occasions to offer our perspective on PIPEDA changes.

Today pharmacists' commitment to privacy is reflected in the professional codes of ethics and standards of practice that guide our profession, as well as CPhA's own privacy code for pharmacists. Given that pharmacists routinely dispense more than 11 million prescriptions each week and they're conducting a range of new, expanded services for patients in almost all jurisdictions, the need for ensuring confidentiality of patients' personal information has never been greater.

Community pharmacists were very early adopters of digital records, having maintained computerized medication profiles for more than three decades. Most of the 600 million prescriptions that are dispensed each year, which is close to $30 billion in spending, are actually sent electronically for claims adjudication by public drug plans or private insurers. So there is a lot of electronic transmission of patients' medication information.

Increasingly, Canadians' medical records are maintained electronically by other health care professionals as well, including physicians' records, lab test results, and diagnostic images. The goal of electronic health records is to increase accessibility and sharing of patient information by those providers who need access to inform patient care and to support interprofessional collaboration.

For example, in several jurisdictions, drug information systems, or DIS, are in place to allow access to a complete profile of medications regardless of which pharmacy dispensed the prescription. This improves safety and efficacy of medications, supports improved prescribing, supports detection of adverse drug events, and deters prescription drug abuse. We hope that in the near future all prescriptions will be electronically created and then transmitted to the patient's pharmacy of choice. With this change to electronic health records comes increased need to ensure that Canadians' private health and medication records are protected.

Let me state up front that CPhA supports the amendments in Bill S-4 as they relate to protecting personal health information. There are two amendments in particular that we want to address.

First, CPhA supports the amendment in the bill in which personal information may be obtained without consent for the purposes of communicating with the next of kin or authorized representative of an injured, ill, or deceased individual.

Pharmacists, as well as any health care provider, may find themselves in the difficult situation of having to deal with patients who may be severely ill, unconscious, or incapacitated for any number of reasons. In such circumstances it may be imperative for the pharmacist or other health professional to immediately contact family members or next of kin to inform them of the patient's condition, or to seek valuable information on the patients' medical history. But seeking permission or consent to contact those individuals in advance may simply not be reasonable nor in some cases possible. This clause would provide pharmacists and other health care providers with the comfort and knowledge that in the case of a severe health emergency they will not be in contravention of PIPEDA for acting in the best interests of their patients by contacting next of kin or authorized representatives.

Second, CPhA also supports the amendment in Bill S-4 requiring organizations that have encountered a privacy breach to report that breach to the Privacy Commissioner and notify individuals, if it is reasonable in the circumstances to believe that a breach creates a real risk of significant harm to an individual.

For pharmacists who access a significant amount of sensitive information related to the medication and health of their patients every day, a breach or disclosure of this information has the potential to put the patient at risk. Patients who are on medications for HIV, mental illness, or infectious diseases would certainly not want all of that information to be known. As defined in the legislation, this risk could include threats to employment, reputation, or relationships. As a result, CPhA believes that, should a privacy breach occur, reporting this breach to the individual concerned and the Privacy Commissioner are reasonable steps to take in order to mitigate any risk that may occur.

● (1125)

It's also reasonable for the organization in question to maintain proper records of these occurrences as stated in the bill.

Although not specifically related to this bill, I want to thank Health Canada for introducing a regulatory change this past summer that will better enable pharmacies to protect privacy. There's a requirement in the Food and Drugs Act that requires pharmacists to maintain up to two years' worth of prescription records, and until last summer the regulation required prescriptions to be maintained in hard copy format even though more and more prescription records are now retained in electronic format. Last July Health Canada reinterpreted that regulation to allow for electronic retention of prescriptions. In addition to being more efficient for pharmacies, electronic retention is safer and more secure from a privacy standpoint.

Thank you, Mr. Chair and committee members, for the opportunity to meet with you today to discuss Bill S-4. I'd be pleased to respond to your questions.

The Chair: Thank you very much, Ms. Cooper.

Now on to Mr Levin.

Professor Avner Levin (Associate Professor and Director, Privacy and Cyber Crime Institute, Ryerson University, As an Individual): Thank you, Mr. Chair. Thank you for the invitation to appear in front of the committee. I apologize that I'm not bilingual, so my comments will be in English. I'm an associate professor and the director of the Privacy and Cyber Crime Institute at Ryerson University and I'm appearing as an individual. I research privacy and I've been privileged to appear in front of the access to information, privacy and ethics committee as well.

I am not going to repeat comments that you heard from earlier witnesses in previous meetings. I take these hearings that the committee is conducting at this time as a sign that the government is interested in considering some amendments to the bill before it proceeds. I would like to reiterate what previous witnesses have said that I think the following amendments should be considered by the committee.

First, I think the committee should consider adding order-making powers to section 12.1 of PIPEDA for the commissioner. Section 52 of the B.C. or Alberta personal information protection act can certainly serve as a model. That does not preclude leaving in the provision for compliance agreements that is in the new proposed bill, which would be the new section 17.1. I'm happy to discuss the reasons for my thoughts on this if we have time for questions later, but other witnesses have already made this point.

Second, I would suggest to the committee that it delete proposed paragraph 7(3)(c.1). That would eliminate the possibility for government institutions to request personal information without judicial supervision. I think that point has also been made by previous witnesses, so I would leave that for questions as well if there's any interest.

Third, I would leave paragraph 7(3)(d) as is. In other words, I do not think the committee should proceed with allowing organizations to share information with other organizations. I think that the committee should leave the investigative body model that is currently in PIPEDA intact and that point has been made.

I would like to spend my time introducing a new point to the committee, as far as I know, and that is regarding the issue of workplace privacy that is in this proposed bill. To the best of my knowledge it has not yet been discussed. Under PIPEDA the personal information of employees of a federal work, undertaking, or business is protected and the collection, use and disclosure of it requires the consent of the employee. That's currently in PIPEDA in paragraph 4(1)(b).

Bill S-4 proposes a new section, section 7.3, that will govern such employment relationships, according to which employee consent will no longer be required. Employers will have to notify employees instead. That's going to be in the new paragraph 7.3(b), but they will be able following this notice to collect, use, and disclose information that, quoting from the bill, “is necessary to establish, manage or terminate an employment relationship.” That's the new paragraph 7.3 (a).

In my opinion, as currently worded, this presents an unfortunate erosion of workplace privacy that ignores previous OPC findings as well as Federal Court decisions. I note to the committee there's a decision from the Federal Court for Eastmond and there's another one for Wansink. I can provide the full citations later. The implications are broader than just for federally regulated employees. Labour arbitrators for those employees who are unionized look to PIPEDA as a guidance and as a source, and to the OPC guidelines. Employers in provinces that do not have private sector legislation look to PIPEDA as guidance even though they do not fall under the jurisdiction of PIPEDA directly.

The proposed amendment appears to follow B.C.'s and Alberta's PIPA, but in my opinion it does not. In those provincial laws—and bear with me, please—the collection, use, and disclosure must be reasonable for the purposes that I've listed. For reference, in the British Columbia act, those are sections 13, 16, and 19. I quote from paragraph 13(2)(b) of the British Columbia Act:

> the collection is reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual.

The new section 7.3 does not refer to the reasonable standard at all. I imagine that's presumably because PIPEDA has built into it subsection 5(3) that says:

> An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

● (1130)

I would hope the committee would follow me in seeing that existing subsection 5(3) refers to the purposes being appropriate to the reasonable person, and it does not refer to the collection or the use or the disclosure as being reasonable. If you want to follow the B.C. and Alberta model, of course the collection and use and disclosure should be reasonable. The purposes of managing, and so on, the employment relationship, needless to say, are reasonable already.

In my opinion the current wording in the bill would allow, to take perhaps a little bit of an extreme example, an employer to install closed-circuit television cameras inside washrooms at the workplace, for the purpose of managing the workplace as long as a notice was posted to that effect. I would argue that for the purpose of managing the workplace and wanting in that case to ensure that facilities are clean and well maintained, doing that is reasonable. But the collection of personal information would not be reasonable in that situation. That is the distinction that I wish to draw to the attention of committee members at this point in time, which I don't think has been articulated up to this point.

I would suggest two simple amendments as a result. One would be to simply add the word “reasonable” before “necessary” so that the amended clause, which would create the new paragraph 7.3(a) would read “the collection, use or disclosure is reasonable and necessary to establish, manage or terminate an employment relationship between the federal...business and the individual”. Alternatively you may wish to consider amending the clause by borrowing language used in Quebec's legislative framework. Section 2087 of Quebec's Civil Code requires employers to protect the dignity of employees, so the committee may wish to consider an alternative formulation such as, “the collection, use or disclosure protects the dignity of the individual and is necessary to establish, manage or terminate the employment relationship”.

I'll make one last point on this, Mr. Chair, before I end my comments. I do think that employees cannot meaningfully consent to their employers' practices in an employment relationship. In that sense I do think that it is useful to move to regulating employers' conduct in those circumstances. I could add more on the issue of consent, but again I think you've heard from earlier witnesses in previous meetings.

I will leave it at that regarding the point on privacy at work. I would be happy to answer questions if there is any time.

Thank you again for the invitation to appear today.

● (1135)

The Chair: Thank you very much, Mr. Levin.

Colleagues, we'll do eight minutes right across the board, beginning with Mr. Daniel.

Mr. Joe Daniel (Don Valley East, CPC): Thank you, Chair. Thank you, witnesses, for being here.

It's obviously an interesting topic and it has raised lots of discussion, input, etc.

Mr. Levin, sir, how do you think that the mandatory data breach reporting would help reduce the risk of identity theft?

Prof. Avner Levin: The mandating of breach reporting is, of course, a useful step that has been called for by privacy advocates for many years. I see it as a necessary step that in fact will bring us in line with other jurisdictions. In the investigations of the House committee on access to information and privacy and ethics, we also raised the point that eventually we would like organizations to see beyond the reporting of breaches that have actually occurred and we would like to have some transparency from organizations regarding attacks that they have suffered.

Obviously the intention is not to have organizations identify their own vulnerabilities but to have organizations in aggregate form, for example the banks through their body, the CBA, report on various attacks, how many have occurred, and where they came from. That is most important, I think, in order to develop public policy.

Without a doubt requiring organizations to start notifying individuals about breaches, as has been suggested in this bill, is a welcome and well-weighted amendment.

Thank you.

Mr. Joe Daniel: Just to follow on from that, do you think we should be legislating manufacturers of computer systems and software to prevent breaches of data?

Prof. Avner Levin: I think if it were possible to achieve that through legislation, then other places would have tried that. But I do think the committee might want to look at the obligations and responsibilities of major companies and major platform providers, which, in the United States, have already started undertaking some responsibility with respect to vulnerabilities in their area. Microsoft, for example, has a threat response centre that looks at and considers threats. Those are activities that I think are appropriate and for which they should take responsibility just because their software is so popular. It's not just Microsoft; you can talk about Facebook and the situations of social media and many other sorts of popular platforms.

● (1140)

Mr. Joe Daniel: Thank you.

Ms. Cooper, obviously the Pharmacists Association plays a critical role in almost everybody's life as I don't see anybody who doesn't take medication of some sort. But would you agree that a regulatory body such as the provincial college of pharmacists should have the ability to obtain information to investigate possible wrongdoing by their own members?

Ms. Janet Cooper: Yes, I would. I think this bill will enable them to access information, and in particular, sometimes you want information that's across the jurisdictions, between the different provinces. Right now many of them are very restricted to only what's happening within their province. It's not just pharmacists. You could have physicians as well, so you have physicians perhaps in one province prescribing through Internet pharmacy, which is not appropriate. It doesn't meet the standards of care. But the pharmacy is dispensing that medication in another province, so it's very difficult to investigate and then to deal with. I think this would enable greater access to information if wrongdoing is expected.

Mr. Joe Daniel: Is your organization forward looking in what's happening with the Internet use of prescriptions, and the lack of borders and boundaries relating to that?

Ms. Janet Cooper: We've been very involved in the whole Internet pharmacy issue for probably at least 15 years because of a lot of concerns. A lot of Internet pharmacies look like legitimate Canadian pharmacies and they're not. They're offshore somewhere and there's no guarantee that the drug you're ordering is going to have an active ingredient in it. It might be counterfeit. It might have chemicals in it that could harm. It is a very concerning situation, one that's difficult to monitor and enforce. Hopefully some of this legislation will make it easier for our regulatory bodies as well as policing agencies and staff to deal with it.

Mr. Joe Daniel: That's excellent.

Your organization in the past has advocated for an amendment to PIPEDA to allow prescribing information to be shared for certain research-related purposes. Does the proposed exception to consent for work product information meet this objective?

Ms. Janet Cooper: Back when PIPEDA was being introduced, there was a lot of concern of how that might impede the day-to-day ability of health care practitioners to work together and care for their patients. A lot was done. There was the whole PARTs tool kit. At the end of it, PIPEDA has not been a barrier. Care, with implied consent and all that, has moved forward.

In terms of the work product, our position has been for some time that de-identified data is really important for researchers to look at: prescribing patterns, prescription drug utilization, those types of things. That may have a prescriber's name attached to it but certainly wouldn't have a patient's name attached to it. It is important that you have access to drug utilization information and the national drug prescription utilization database that CIHI maintains that gets information coming in from the provinces on that as well.

Mr. Joe Daniel: So forgive my ignorance about your industry or your side of it, but what research are you doing with all this data?

Ms. Janet Cooper: We are not as an association but you have a lot of universities, agencies, that are looking at appropriate medication use and safety. So to get that data in on prescribing patterns and utilization is really important. We're spending over $30 billion and almost half of that is paid for through the public purse for prescription drugs. But there are lots of concerns: are medications being taken appropriately, prescribed appropriately, monitored, are they safe, as well as prescription drug abuse. We also have a lot of costs related to less than appropriate medication use. It's really important that there's research to look at safety, efficacy, those issues.

● (1145)

Mr. Joe Daniel: Okay, thank you.

Now for the folks from the Public Guardian and Trustee side, you have a really tough role to play. I think some of the numbers that came up was 1,600 people. Is that the tip of the iceberg or do you think you're covering most of the abuse that's taking place at these financial institutions to people who are not necessarily able to understand what's going on?

Ms. Catherine Romanko: Thank you for the question.

I do think it's the tip of the iceberg. There are several factors to consider. Number one is that public awareness of financial abuse, or the risk of financial abuse, is growing. I think we've seen this on a national level and certainly provincially. Financial institutions are increasingly raising this issue and training their staff. I think that as public awareness grows, there will be more reporting.

The other factor, particularly in British Columbia, is the changing demographic that we see with an aging population. We know from statistics that the incidence of dementia once someone reaches the age of 85 is significantly increased. We know generally, without getting into statistics, that the aging population tends to become more vulnerable. Not everyone does but many do. It's the vulnerability, not necessarily incapacity, that can lead to potential abuse.

I think it is the tip of the iceberg. I don't think that even now we are receiving all the reports of abuse. I do expect that we'll see an upward trend.

The Chair: Thank you, Ms. Romanko, that's all the time that we have there.

Now we go to Ms. Nash.

Ms. Peggy Nash (Parkdale—High Park, NDP): Thank you to all the witnesses for being here today. This certainly is a very far-reaching and interesting topic.

Professor Levin, I'd like to start with you. Although this wasn't the focus of your presentation, you referred to it. We did have several witnesses testify about the anti-privacy provisions in this bill, specifically the clause that states that information can be disclosed without the knowledge or consent of an individual if that information is being used to investigate a breach of an agreement or a contravention of the laws of Canada or the province. Do you think that this clause is necessary, or is it overly broad? Do you think it complies with the Spencer decision?

Prof. Avner Levin: Thank you very much for the question.

I will repeat what earlier witnesses have said and I'm in agreement with them. I think the clause as written is overly broad. I think it corrects something that, in fact as this committee heard from the bankers, does not actually need correction. The bankers who appeared in front of the committee were quite happy with the investigative body model that they have. They have well-reputed investigative bodies to research fraud and those issues that are concerning to all Canadians in terms of identity theft.

I think other witnesses have also noted that to just look at what's happening in British Columbia and Alberta in terms of similar provisions is misleading because they don't deal with the same type of organizations, namely the big telecommunication and Internet service providers that fall squarely under the jurisdiction of PIPEDA. That's why I recommended that the committee should not tamper with it. It should leave the existing model that exists in PIPEDA as it is and not proceed with these amendments.

To address your other point, certainly the spirit of Spencer is that Canadians have expectations of privacy in all of this information. As somebody who researches privacy, to see a bill come forward with many good provisions about privacy but also many exceptions that allow people to do things without consent and without agreement, to me that is problematic when we got a signal this summer from the Supreme Court that everybody has reasonable expectations of privacy in that kind of information.

Ms. Peggy Nash: Thank you.

I want to ask you about breach notification. The threshold is pretty high, it's “a real risk of significant harm”. Do you think that is the right threshold? We've had some witnesses suggesting a two-step system where the Privacy Commissioner is informed of all breaches and then there is a decision about when an individual is notified about a breach. Do you think that the way it is structured now under Bill S-4 it's leaving these decisions to industry itself? Is that the right approach?

● (1150)

Prof. Avner Levin: It is leaving the decision to industry itself but I think the more important issue is that the standard has been set at a certain level. I know there has been a lot of debate over the appropriate wording and the standard had been set finally at a level that is fairly high.

In my research I'm just as concerned with attempts of breaches as actual breaches. My concerns are also about organizations in aggregate form not disclosing information about attempted attacks that they have suffered and what we call attack vectors, where do the attacks come from. A lot of what we often tell people.... For example, the banks will often always tell customers that they have to protect their passwords, etc., but we don't have good information as to where the attacks are originating from. They could be originating from overseas, from hackers, and not from negligent customers.

Attacks are just as important as these actual notifications in my own research and my own work, and that's where for me in the system, at least as you see it in other countries, people do get notified. Whether that's going to offer the best protection for Canadians at the end of the day I think there may be further actions that are required perhaps down the line as you see if this system is working effectively or not. I am concerned that right now there's nothing about potential attacks but only actual breaches.

Ms. Peggy Nash: Thank you.

I want to ask you about information sharing by companies in a prospective business transaction, which would be allowed under Bill S-4 without the knowledge or consent of an individual. Do we need this clause and does it strike the right balance around privacy and the need for businesses to have certain information?

Prof. Avner Levin: As I understand this clause, it was at the request of businesses in terms of mergers and acquisitions where they felt that to go and technically request the consent of each customer when a merger is contemplated or something of the sort would be cumbersome and the customer's information is not used in any kind of meaningful way. It's just handed over from one party to the other. That is a provision that exists in British Columbia and Alberta, in the same language, and it hasn't caused significant concerns in terms of how it applied over there.

For me that is not in itself a troubling proposition. It facilitates business. Hopefully people won't look and find some unexpected loopholes in it, because the purpose of it is pretty straightforward as I understand it.

Ms. Peggy Nash: Thank you.

My time is running out, but I wanted to ask Ms. Cooper about pharmacists.

There is a concern about the work product, that sometimes a doctor's prescribing history has been made available to pharmaceutical companies for marketing purposes and that they're buying that information from pharmacists. Currently, they're having concerns in the U.S., for example, that this could lead to targeted marketing, that it could increase health care costs, and in fact that information is getting shared without the knowledge or consent of the doctors.

I know in Quebec they have a doctor opt-in provision and in B.C. I think they have decided not to allow this practice. Can you comment on that? Is it a concern that pharmacists have?

Ms. Janet Cooper: It is a concern. We have a position that we support the collection of prescribing information but it should be de-identified of the prescriber as well as obviously the patient.

We hear some of those stories as well where it seems they get down to such a narrow postal code and there might only be two specialists so it's pretty obvious that these are the physicians who are prescribing. It is influencing the drug reps who are going in and talking to the physicians and the physicians are surprised that this much information is available.

It's really important that this information be collected to ensure that there's appropriate utilization of medications. What you have now are the representatives going in and they're prescribing usually their new products. There may be an equally effective and far less expensive generic product on the market that really should be used because it's been around longer and it has a lot more safety information about it, so you really don't want to have situations where that very targeted marketing and information is that widely available.

We certainly see that it's important to inform appropriate prescribing medication use and researchers to do that, but not for the marketing purposes that we hear about.

● (1155)

The Chair: I'm afraid that's all the time we have.

Now we'll go on to Mr. Warawa.

Mr. Mark Warawa (Langley, CPC): Thank you, Chair.

Thank you, witnesses, for being here.

I want to focus my questioning on how the digital industry has so dramatically changed since PIPEDA first became law in 2000. I believe that things have changed dramatically since it came into effect. It actually came into force from 2001 to 2004, over three years. Then, as is normal, there was a judicial review, a parliamentary review, and that started in 2006-07. I think some of you have been involved with that and have provided submissions or have testified.

Bill S-4 contains I think important updates that relate to what we saw when it was established in 2000. In regard to what's being proposed now in Bill S-4, the world has changed. Technology has changed dramatically. That includes the number of people who are using digital technologies for emails, banking, and so on.

We've heard from you. We've created Bill S-4. It provides important updates to current private sector privacy laws that will help protect consumers with regard to their personal information, whether it's been stolen or lost.

There is currently no legal requirement for a business to inform consumers when there has been a data security breach. A business could be hacked and decide right now not to inform customers, but the changes in Bill S-4 will compel businesses to report when hacked and will impose fines of up to $100,000 per individual if the business fails to notify the customer.

It also provides some very important focus on protecting the vulnerable, both the youth and our seniors.

Ms. Romanko, you touched on that, as did Mr. Brown, and that's the focus of your organizations.

The Bankers Association was one of the many that really supported Bill S-4. They applauded the amendments in the bill that will allow banks and financial institutions to advise public guardians, law enforcement, or family members when they have evidence of financial abuse. I think you touched also on the abuse that may be coming from family members. The banks would now have the discretion in regard to how to deal with these serious situations and protect the vulnerable. That does not exist now.

We also heard from the Privacy Commissioner about the tools necessary for the commissioner to do their job. There was not adequate time for them to be able to act. Now, with the changes in Bill S-4, that would change.

If you could, just touch on how things have changed and on these changes that have been now incorporated in Bill S-4 to update PIPEDA.

Ms. Romanko.

Ms. Catherine Romanko: Thank you.

Yes, I would be happy to do that. Of course, my comments are very narrowly restricted to the ability of financial institutions to report.

The Public Guardian and Trustee of British Columbia was working closely with the Canadian Bankers Association back when these proposed amendments were first suggested. We were very much in support then of allowing an amendment that would enable financial institutions to report proactively, not just when there was an actual contravention of the law.

It is in that proactive measure that we think vulnerable persons are better protected. Then the responsibility for investigating falls to the provincial bodies, the public guardians and trustees, to do what they already are able to do under the law.

The missing piece was the proactive reporting. Bill S-4, in the provision in proposed paragraph 7(3)(d.3), I believe will accomplish that. I believe that is a positive measure.

● (1200)

Mr. Mark Warawa: Mr. Brown.

Mr. Douglas Brown: I can take that even a step further.

Prior to my appointment as public guardian and trustee, I was director of enforcement for the Manitoba Securities Commission for about 12 years. The trends you have seen over the last two generations are people becoming more involved in their financial management. It's not just simply savings accounts and bank accounts anymore. You have people who are investing in mutual funds and other investment products. You have a more complicated landscape out there, which, if you take the negative view, probably leads to more opportunities for abuse of an individual, for example, if an individual is trying to manage money in different ways than they have in the past.

The other thing—and we were briefly talking about it before we came in—is the change, particularly in the banking industry to electronic banking, Internet banking. There is a move away from direct physical contact at a branch, which you would have seen a generation or two ago. That also creates a complexity in the situation that you're not going to have.... Whereas 20 years ago you'd have your local branch manger, whom you probably saw every couple of weeks just because you would be visiting your branch, that sort of contact isn't there anymore.

As we go further and further, with younger generations it's going to even become more pronounced. That doesn't change the need for this legislation, the need for the reporting. I think it's going to force us to adapt to those situations in our various roles to try to figure out ways that we can still identify potential abuse and report it under these new ways of delivering the service.

Mr. Mark Warawa: We have nine weeks of work here, including the constituency weeks, and a lot of work to do before this Parliament wraps up.

Is it important that we pass Bill S-4 within this Parliament, or do you think we should be waiting? Will we leave people vulnerable if we don't pass S-4?

Mr. Douglas Brown: People are vulnerable by not passing it.

We have organizations, as defined in that legislation, that don't feel they have the legal ability to report situations where they themselves are identifying possibilities of abuse. In terms of public protection, I'm not sure why we would allow that to stand.

With regard to any of the comments I've read on the bill, I think they can be dealt with in regulations for the most part. Things like defining governments organizations or government institutions can be dealt with in the regulations.

I think this is an opportunity to at least take that first step, put some protections in place, and then, as in any piece of legislation, see how the actual utilization of the legislation rolls out. We could always decide on amendments in the future.

The Chair: Thank you very much, Mr. Warawa.

We'll go to Ms. Sgro now.

Hon. Judy Sgro (York West, Lib.): Thank you very much, Mr. Chair.

Welcome, and thank you for sharing some of your time and your insights into this issue.

Professor Levin, the penalties we're talking about go from $10,000 and up for people who don't report.

There seems to be such an easy way to have breaches of people's privacy today. Constantly, everywhere you go, you're being asked to tick a box that says “I agree”. A piece of software that I looked at yesterday had seven pages. Now I'm not going to read those seven pages—I'm just being blunt—and I don't think anybody else is who's not some high-tech person who has a specific reason that they're looking at that. However, in order to have access to that particular program, I scrolled through the seven pages and clicked “I agree”. I tend to think that's what a lot of people do.

Could you comment on that? I mean the object with Bill S-4 is to make privacy legislation better and strengthen people's confidence in it. I think that's what we all want to do.

Prof. Avner Levin: Thank you very much for the question.

I think the real issue is what has been happening with the digital economy and with services, as you can see. Certainly, since PIPEDA came into force, the idea of consent has changed. Instead of protecting us as individuals, it provides companies with loopholes, these seven pages of legalese, to say that we as individuals have agreed to all further collection, use, and disclosure practices.

The idea that, in this day and age, we can provide meaningful consent is broken, and has been for quite some time. That's why, in the academic world, if we're talking about a privacy framework for the 21st century, there is a lot of thought as to whether we shouldn't be moving beyond just focusing on consent as a gateway, such as saying that if someone consents then everything is fine. We should really be restricting what companies do with the information they collect. We should see a lot more regulation of uses and disclosures, not enabling of organizations to say, “Well, I've got somebody ticking a box over here, therefore I can go ahead and do whatever I want.”

This is a serious concern, especially when you're talking about this new kind of big data analytics in which companies are trying to collect a lot of information, do what we call free-form analysis, look for correlations, and do the type of predictive analytics that then make the headlines. For example, Target sent a notice to the family of a teenager that their daughter was pregnant. The father didn't know, but Target staff knew because they punched the numbers.

Regulation of use is what is required in this day and age, not just focusing narrowly on consent. Organizations will find the loopholes. They'll use legalese and write long agreements. That has not been helpful so far.

● (1205)

Hon. Judy Sgro: Do you think that there are opportunities for us to somehow tighten up that particular area in the regulations?

Prof. Avner Levin: If not in this iteration of the bill, certainly I would want to see it in regulation, because the bill in its current form is still under the old model. Make no mistake, while I'm stating these opinions as an individual, privacy commissioners will tell you how important consent is. I don't disagree with the idea in principle. It is just to say that as a practice it's not working. We need to think about how we can bolster and support it. Maybe regulation is the proper tool for that.

Hon. Judy Sgro: Could we possibly do it with amendments to Bill S-4?

Prof. Avner Levin: Well, if you really wanted to contemplate that, I would introduce restrictions on how companies use and disclose information, so that it's not as if consent is the gateway to an agreement with you where you've agreed and anything goes. Rather, there would be only certain purposes that they would be allowed to use that information for.

There are many ways in which you could, maybe through regulation, ask companies to touch base with a customer at key points, and say, “I want to do this with your information now. Do you agree at this point in time, yes or no?” Technologically, these tools are all available, but we don't have the legal framework that will force companies to do that.

Hon. Judy Sgro: In the penalty process that requires companies to report all violations, all breaches, one of the concerns from some of our witnesses was that companies are not going to do so. It will be too cumbersome. They're not going to report all the breaches. They'll take a chance on not doing that and possibly pay a fine because there are so many breaches that are happening on a daily basis.

Prof. Avner Levin: In terms of enforcement, part of the problem that we have concerns the role of the commissioner. The commissioner, who does not have the ability of other commissioners to issue orders to companies, is not viewed by companies, and typically by small businesses....

We see a lot of non-compliance simply because the consequences in their mind are not as real as, say, a health and safety violation for the municipality. We need to see more powers, so that the commissioner is actually treated like a regulator and not an ombudsperson. The old model was that the commissioner was an ombudsperson resolving disputes between customers and companies. I think we need to see the commissioner moved to regulator.

If we give the commissioner powers to enforce these things, large and small businesses will take that more seriously.

Hon. Judy Sgro: Very much so.

Ms. Cooper, would you like to add any comment in those areas?

Ms. Janet Cooper: Yes.

Certainly as a professional association representing pharmacists, we find some of this discussion is outside of our mandate and my particular expertise, unlike Dr. Levin's. But I share those concerns, even more just as a Canadian, that we're signing off on a lot of stuff when we tick those things.

I look at the younger generation. I was recently at a Canada Health Infoway meeting, and they had some research done with Canadians and focus groups. I was surprised with the lack of concern that many Canadians have about their private information. For example, they just assume that every pharmacy in this province...you know, the Shoppers Drug Mart here shares it with the Shoppers Drug Mart three blocks over. They don't share it, but people assume it and they expect it.

I think societally we have some real challenges, and we're ticking off a lot of stuff. I would personally agree that we need to look at better regulating what companies can do with this data, because there's a lot of information that's coming in at point of sale, Internet sales, Google searches, and all that type of thing, which we need to be looking at.

I really couldn't comment on whether it should be within the legislation or regulations related to this, but I share the concerns.

● (1210)

Hon. Judy Sgro: It needs to be handled somewhere along with this package.

Ms. Janet Cooper: Yes.

Hon. Judy Sgro: Okay, thank you.

The Chair: Thank you very much.

Now we'll go on to Ms. Gallant.

Mrs. Cheryl Gallant (Renfrew—Nipissing—Pembroke, CPC): Thank you, Mr. Chairman.

My first question goes to Ms. Romanko. Does financial abuse that is reported to you include the sale of vehicles to people suffering from the effects of dementia? For example, if we have an elderly person who is sold a car and that person can't drive or doesn't have a licence, can people report that to you as financial abuse?

Ms. Catherine Romanko: They can. That case that was recently in the media actually did come through our office in a very preliminary way early on. The circumstances could be reported as abuse, but when it's a commercial operator, the chances are the report would go to the police rather than the Public Guardian and Trustee to see whether the transaction was legitimate, and whatever. It's unlikely that we would be involved from the perspective of pursuing the vendor of the vehicle, the commercial operator, but rather protecting the adult.

What we might do in those circumstances is examine the affairs of the adult to determine whether there are supports in place and ways to protect the adult. Does the Public Guardian and Trustee need to become involved on an ongoing basis as a committee, for example, to manage the affairs of the adult?

There are certain types of situations that simply can't be avoided. People who have legal representatives but are incapable may still enter into transactions without the vendor knowing that the person is incapable, and presumably, they've entered into a situation that may not be in their best interests. There are provisions under British Columbian law that would perhaps negate that transaction to protect the vulnerable adult, but there are some things that are really difficult to protect. Our office would be involved only from the perspective of protecting the adult, not necessarily undoing the transaction or pursuing a vendor.

Mrs. Cheryl Gallant: Okay. If there were a financial institution involved or a lending practice, has it been your experience that any financial institutions reported abuse when it involved a loan as opposed to a withdrawal of deposit?

Ms. Catherine Romanko: The loans haven't been particularly our experience, unless it is a situation where you have a vulnerable adult come into the bank with a new person in their life and unusual withdrawals are being taken and loans to this new person. That sort of thing is reported to us. With respect to loans that are made by the bank to vulnerable adults, that is not something I'm referring to.

Mrs. Cheryl Gallant: Okay, thank you.

Ms. Cooper, are you or your membership in the Canadian Pharmacists Association aware whether or not they've ever suffered a data breach?

Ms. Janet Cooper: I'm not aware of that information being disclosed. I think there have been some extremely isolated incidents —you know, a member of the pharmacy staff might have looked up a patient record—but there are really good processes in place to identify that. In provinces like British Columbia, there is a province-wide information system of all the medications that every pharmacy can get. The same as breaches within a hospital, or any provider, some of that is being detected. How much it's reported, I don't know.

But in terms of prescription information being breached, I can't recall that having happened in spite of having electronic records of prescription data for about three and a half decades.

● (1215)

Mrs. Cheryl Gallant: Do pharmacies conduct audits of who is accessing...? Can an employee, for the sake of whatever, snoop on a client's profile to see what medication they are on?

Ms. Janet Cooper: In the provinces that have a province-wide drug information system, it's a government system, so they are auditing that. They can identify the people who are accessing when they shouldn't be. That's not unique to pharmacy, either.

Mrs. Cheryl Gallant: Would you be able to explain how prescribing information can be used for research that would benefit patients? You used that phrase earlier in responding to a question, but would you follow through on that concept and explain to the people here how patients in general would benefit from that type of prescribing-pattern research?

Ms. Janet Cooper: It's all part of post-marketing surveillance to look at a lot of safety information. Before drugs come on the market, they're tested in a fairly narrow, often homogeneous group. When they come out on the market and you're using them in pediatrics or the elderly or people with kidney dysfunction, they probably haven't been tested in some of those populations, so it's really important to get that information.

Most drug plans, in particular the government drug plans, have formularies and they have restricted access. They want to know that these drugs that are restricted because of either cost or safety concerns are being used appropriately and for the right patients. Without collecting that information, you wouldn't be able to research any of that.

Mrs. Cheryl Gallant: I don't see how you're able to connect the dots with respect to prescribing patterns when you don't actually have the knowledge of how that patient is reacting to what's prescribed.

Ms. Janet Cooper: In terms of the clinical outcomes for that particular individual?

Mrs. Cheryl Gallant: What you just described requires knowing how the patient is being affected by the medication. Based on what is on a prescription order, that's not indicated.

Ms. Janet Cooper: You start to get more of that with better integration of adverse drug reaction reporting and clinical outcomes. British Columbia has a pretty impressive integrated.... They can look at cardiac outcomes based on utilization of cardiac medicines, that type of thing. These are all very highly educated researchers. Most of them who are doing a lot of this research are on faculties of medicine or pharmacy.

Mrs. Cheryl Gallant: So you're not comparing actual outcomes per patient; you're comparing statistics to statistics.

Ms. Janet Cooper: That's right. When you look at clinical research, it's the number who have been treated and what their outcomes are compared to a control group that's not on medications or on a different medication, that type of thing.

Mrs. Cheryl Gallant: Thank you.

The Chair: Thank you, Ms. Gallant.

Now on to Ms. Borg.

[*Translation*]

You have eight minutes.

Ms. Charmaine Borg (Terrebonne—Blainville, NDP): Thank you, Mr. Chair.

I thank the witnesses very much for being here today.

My first question is for Mr. Levin.

I had the opportunity of hearing your testimony at the Standing Committee on Access to Information, Privacy and Ethics. You said that businesses had to be motivated to protect people's personal information.

In my opinion, Bill S-4 is an improvement, but it does not go far enough to encourage companies like Google and Facebook to properly protect individuals' personal information. You mentioned briefly that you were in favour of compliance agreements, but you added that they should confer more powers.

Could you provide some further explanations on that?

[*English*]

Prof. Avner Levin: If I understand the question correctly—and thank you for the question—it was asking what we need beyond the compliance agreements that are currently in the bill.

I think what we need is the power, at the end, for the commissioner to make an order and instruct those companies to comply with whatever it is that the commissioner has found. You have a process of discussion and you have findings and you have a compliance agreement, but what we have right now is that at the end of the day the commissioner can then go to court and request an order.

We have seen an excellent example with the research that was done by the commissioner with respect to Facebook a few years ago —very thorough research by the assistant privacy commissioner, currently the privacy commissioner of British Columbia, into Facebook—with lots of media attention, lots of findings, lots of recommendations. Then Facebook says that's wonderful and moves on and keeps doing business as usual. They disregard Canada and they disregard the regulator, because the regulator doesn't have the power to order them to comply with any of those, and the only option is maybe to take them to court.

In order for big businesses to take the Canadian environment seriously, the commissioner has to be able to tell them at the end of the day that they have to comply with a certain finding or a certain request. What is baffling to me is that this is very common in data protection regimes. You see that they treat Europe differently as a result, because the commissioners there have the ability to regulate and make orders. You can see how they treat even provincial commissioners differently, because they have within their provinces the ability. The only outlier is the Privacy Commissioner of Canada.

I don't understand what the compelling reasons are to make an exception in this case, so that the Privacy Commissioner of Canada cannot be given the powers of making orders that all the others have.

● (1220)

[*Translation*]

Ms. Charmaine Borg: Thank you very much.

I would also like to raise the issue of consent, which is I think of concern to all of us. The fact that there are 10-page forms that people cannot read is indeed very worrisome. Bill S-4 at least sets the stage for limiting the circumstances in which consent could be considered valid. This is in clause 5 of the bill. Several witnesses made different comments on that clause.

Mr. Levin, Mr. Brown and Ms. Romanko, since you spoke of the most vulnerable populations, I would like to ask you whether in your opinion this clause is appropriate as it stands, or whether it should be amended. If so, what would you propose?

[*English*]

Prof. Avner Levin: I think the clause is good because it provides greater clarity. If we are going to stay with the regime of consent, you want something that is clearer rather than more vaguely worded. My broader concern about where Bill S-4 is right now in 2015 is that we have seen that all of these ideas of consent are not actually effective. We need to see much stronger protections in other areas, in terms of regulating use and disclosure.

But I think the clearer language is a very welcome step, from my perspective.

[*Translation*]

Ms. Charmaine Borg: Mr. Brown, Ms. Romanko, do you have any comments to make on the content of the article?

[*English*]

Ms. Catherine Romanko: I don't think I can comment on the clause, but I would say that one thing to bear in mind is that someone who is not mentally capable at law cannot provide valid consent. What protection that adds is probably none.

[*Translation*]

Ms. Charmaine Borg: Very well, thank you; that is a good point.

I imagine you were going to say the same thing, Mr. Brown.

Mr. Brown, Ms. Romanko, I would also like to ask you a question on the proposed amendment to allow the sharing of information without consent in cases of financial abuse. The provision reads as follows:

> (iii) it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the ability to prevent or investigate the abuse;

I don't know if you will be able to answer my question, but I can't think of a situation where the person's consent might have an adverse effect on the investigation. Based on your experience, perhaps you could tell me when this provision might apply.

[*English*]

Mr. Douglas Brown: When you see cases of financial abuse, quite often the first step is that the individual who is doing the financial abuse is gaining the trust of the person we're trying to protect. The reason that this clause is important is that quite often you will have a situation—say it's a senior who goes to a bank—in which, if you inform the individual that "we have a concern that you're being financially abused", the first person the senior will go back to is the person who is actually doing the abuse. In order to break that cycle, it's very important in some situations for the financial institution to be able to report to the government institution, so that the investigation can be done outside the influence of the person who may very well be perpetrating the financial abuse.

● (1225)

[*Translation*]

Ms. Charmaine Borg: Thank you.

I'd like to go back to the issue of consent. I know I am bringing it up a lot, but it is a big concern.

One witness suggested that we limit or prohibit communication when seeking personal information regarding minors or seniors. This is similar to what Mr. Levin proposed. In my opinion, this might prevent people from having access to certain services. I don't know how we could deal with this question.

I would like to hear your comments on this, Mr. Levin or Ms. Romanko.

[*English*]

The Chair: Let us have a comment, as brief as possible, from one person.

Ms. Catherine Romanko: I'm not sure I can comment on that.

Prof. Avner Levin: I would just like to say briefly that this is an issue that is outside of the bill, because it has to do with how you identify and de-identify data. It gets into technical issues and that is a whole other separate conversation.

The Chair: Thank you very much, Mr. Levin.

We'll now move on to Mr. Lake.

Hon. Mike Lake (Edmonton—Mill Woods—Beaumont, CPC): Thank you, Mr. Chair.

Thanks to the witnesses for being here today.

It's interesting that as we do legislation there always seem to be three categories of potential amendments. Everybody has suggested modifications to the legislation. You either have people who want to add something that isn't in it that they think should be in it; or you have people who take a look at changes that are being made and don't agree with them and want them not to be made; then, there are some technical changes, as almost always someone will suggest some kind of technical wording.

It's interesting that the first category in a sense seems to fit, Catherine, most of what you have had to say. You talk about some clarity around provincial authorities, but I would argue that the legislation, in I think proposed subsection 26(1), says:

> The Governor in Council may make regulations for carrying out the purposes and provisions of this Part, including regulations

This includes, as it is written in the existing act:

> (a) specifying, by name or by class, what is a government institution or part of a government institution for the purposes of any provision of this Part;

So we have the ability to do that through regulation and I think you would be satisfied with that as a mechanism. You just want to make us aware of the need for some clarification there, I believe. Is that right?

I was interested in your second recommendation, deleting “next of kin” as your number two area of refinement.

Why would you do that?

Ms. Catherine Romanko: The deletion has a two-fold purpose.

“Next of kin” don't have any entitlement under law to personal information. “Next of kin” are also often the perpetrators of abuse. Including them as one of the options for financial institutions to report to perhaps tips the balance against protection and the privacy rights. You're balancing the adult's right to privacy against the need to protect, and I think the balance is tipped.

Hon. Mike Lake: I find it interesting that you would give rights for an appointed guardian to be informed about something, but not for an actual family member, which is an interesting challenge. I say that because I have a 19-year-old son with autism—full disclosure. If someone got close to him and were somehow financial abusing him and taking advantage of him, I would want to be the person called to find that out first, if I didn't know it. It would seem odd that we would exclude me from that list of people who would be informed.

Ms. Catherine Romanko: Right. I appreciate that, and in most instances, that....

I suppose one of the balances here is that if the language is left in the bill, the understanding then would be that the financial institution would have a broader range to exercise its discretion, and presumably would not report to someone they suspected was the abuser. I still think there is a risk there. I think there is a distinction, as you raised, with respect to the authorized representative, in the sense that an authorized representative would have legal authority—granted either by the individual themselves, when they made a power of attorney, or when they made a representation agreement under British Columbia law, or when they were appointed by the court to act.

In those instances, they're guided by law. They have a fiduciary relationship with the adult. There's an extra set of rules governing their behaviour. Yes, they too go off the rails. Yes, they too are sometimes the perpetrator. But I think at least there's greater.... Again, it's a question of balancing the right to privacy with the need to protect the adult who may be vulnerable. It seems to me there is greater justification to allow a reporting to someone who has legal authority than to someone who has no legal authority to receive the information about the adult.

That said, I think it is more important that this provision proceed than the amendment to next of kin be made. In other words, I wouldn't want to stop that section from being enacted simply because of the next of kin issue.

● (1230)

Hon. Mike Lake: Okay.

Your third point was on neglect and self-neglect. I think that sort of fits into that first category of things that might be nice to consider down the road at some point, but right now, in the interest of passing important legislation, we can probably have that discussion a little bit later.

I guess further to that, Mr. Levin, I think your first point—I always have a tough time jotting down all the points and getting them bang on—was about adding order-making powers for the commissioner. It's not in the legislation at all, not a change, but just something you would add if you were writing legislation. It's something that you would like to see added.

You know, we've taken pretty significant steps forward without that specific provision in the area that you're concerned about. Is that accurate?

Prof. Avner Levin: Yes, you gave them the ability to do compliance agreements, which I think is a lot better than what they have right now, which is nothing.

Hon. Mike Lake: But you would argue that maybe the next time this discussion is happening about this particular legislation, we might want to consider order-making powers.

Prof. Avner Levin: Well, I would argue that you should consider it now. You can decide what you will decide.

Hon. Mike Lake: Okay. Sounds good.

You also I think talked about deleting paragraph 7(3)(c.1).

Prof. Avner Levin: Yes.

Hon. Mike Lake: Again, that's not something new in the legislation. That's something that's already existing in the legislation. If you were the minister, you would be moving to make that part of what we're doing. You'd add that to the steps being taken.

Prof. Avner Levin: I would delete it because of the Spencer decision that happened in the summer. I would make it clear that the government wants law enforcement agencies to get judicial authorization when they request information, because that's how I understand the Spencer decision.

Hon. Mike Lake: So I imagine that, moving forward, regardless or whether this legislation passes or not, you'll be advocating for that in the next iteration. Okay.

Was it paragraph 7(3)(d) that you said to leave as is?

Prof. Avner Levin: Yes.

Hon. Mike Lake: Could you maybe explain that?

Prof. Avner Levin: Right now there is this investigative body model in which the banks, typically, that are concerned about fraud —they've presented in front of you—have these investigative bodies, and then they share information through the investigative bodies. That's how they wrap their heads around these issues of fraud.

The bill is going to remove that and have these other provisions in which organizations can interchange with other organizations on the information. The concern is that it's too broad, that it's not actually what industry is requesting and it opens the doors to what we're seeing right now in the area of copyright—companies abusing the legislation and sending people thousands of notices, telling them they have to comply with Canada's Copyright Act or else.

It's an area where we don't want organizations having what I would call the “unfettered” ability to go to other organizations without the consent of the individual just because they think an agreement has been breached.

Hon. Mike Lake: But is there any...? This is a system that exists, I believe, in B.C. and Alberta, right?

Prof. Avner Levin: Correct.

Hon. Mike Lake: I believe that system has existed for a long time. What evidence is there that this has resulted there?

Prof. Avner Levin: Well, they don't have any Internet service providers, and mostly the concern here is around Internet service providers.

Hon. Mike Lake: It's very specific to Internet service providers?

Prof. Avner Levin: Yes—which this legislation regulates.

Hon. Mike Lake: Okay.

The Chair: Thank you very much, Mr. Levin and Mr. Lake.

Madam Papillon, you have eight minutes.

[*Translation*]

Ms. Annick Papillon (Québec, NDP): If possible, I will let my colleague ask the first question.

● (1235)

Ms. Charmaine Borg: I'm going to ask another question, and then I will yield the floor to Ms. Papillon.

Mr. Levin, in reply to the question put by my colleague Ms. Nash, you said we would need to have some idea of the privacy breaches which might occur, and not only of those that have already occurred

How could such a system be set up? It seems to me that this is something that we could consider in the future. How could we include the system in the act or in the mechanism regarding breach of privacy? Could you elaborate on that?

[*English*]

Prof. Avner Levin: Thank you for the question.

I think this is the classic situation in which the banks don't have to disclose their own vulnerabilities, but they can, in aggregate form through an organization like the CBA, report all the various attacks that have occurred in a certain time period and where those attacks originated from. They'll say that they've had all of these malicious people from the outside or they've had malicious insiders. The Bank of Nova Scotia has been sued in a class action lawsuit because of the actions of a rogue employee. That was not audited properly by the bank in terms of accessing personal information.

We need to know that not just when it comes up and somebody sues, but in aggregate form so that we can develop policy accurately and so we can ask where the focus should be. Should we be investing in protecting our national infrastructure, and the banks are part of that? Should we be telling customers to keep their passwords safer and so on and so forth?

These are basic questions that we don't have answers to. If we got them in aggregate form about various industries, it would be very helpful. We don't have that right now.

[*Translation*]

Ms. Annick Papillon: I would like to get back to bill S-4. As we know, this bill would give the Privacy Commissioner new powers to conclude compliance agreements with organizations. However, given that there will likely be insufficient resources at the Office of the Commissioner, do you not think that he may be overwhelmed by the task, and that every breach that occurs will be submitted to him?

M. Levin, could you answer that question, please?

[*English*]

Prof. Avner Levin: I know that the committee asked the commissioner about the resources and received I think a very diplomatic answer in response. I think this is part of the transition that office has to go through, looking back on 15 years of private sector legislation.

When I hear that the commissioner is repeatedly talking about education, it disturbs me, because regulators don't spend a lot of time educating. You don't hear the CRTC talking about educating. You see them making the rules and changing the landscape for the businesses they're regulating. I think the same thing has to happen with respect to the Privacy Commissioner. They need to move to the model of regulator. If that means they need to move resources internally or get additional resources externally, then I think that's what has to happen.

But if we care about personal information protection, we must have an effective national regulator. Right now, we don't have that. As we've said before, we have an ombudsperson who deals with trying to solve complaints.

[*Translation*]

Ms. Annick Papillon: I appreciate your comments very much.

Somebody is going to have to maintain a record of the breaches for the Office of the Privacy Commissioner of Canada in order for him to be able to verify them. However, if the commissioner does not have the necessary resources, I fail to see how he will be able to do that. In that case, these records may be of no use.

I will continue in this vein and ask you for your opinion. What would the solution be in that case?

[*English*]

Prof. Avner Levin: From my perspective, and just sort of blue sky, obviously you need to bolster the resources of the Privacy Commissioner to deal effectively with these issues, just as when Canada's anti-spam legislation was passed and in Canada you needed to bolster the ability of that department within the CRTC to control that.

I don't know if it's been done sufficiently or not, but to me, in legislation, you set the mechanism of what you want the organization to do, and then the resources just naturally follow from that. Why give somebody the powers and then not give them resources to do their job? To me that doesn't make any sense.

[*Translation*]

Ms. Annick Papillon: That seems very logical to me.

What would happen if a business simply did not declare its breaches of data in order to protect its reputation? In your opinion, would the fear of contravening the law's requirements be sufficient to ensure that businesses will be diligent in this regard?

● (1240)

[*English*]

Prof. Avner Levin: I don't want to tar all the companies with the same brush. I think we have a lot of organizations in Canada that try to do the right thing. Certainly the big organizations that are Canadian try to be in compliance with legislation and are very concerned. That's why you see them appear here in front of the committee trying to advocate for this and that point of view. I don't want to say that people don't want to be in compliance, but we could be in situations where, again, just because of the force of business and what's a pressing issue upon them, they deal with some things more seriously than they deal with others because of the penalties they think will happen or not.

The legislation gives them the discretion to decide as it is, so they have the power to just make the decision. I think the jury will be out on whether that is an effective system or not. Time will tell. It may be one of those things that you do have to revisit and say it is not working properly and we need to move to a two-stage system, or we need to set the threshold at a lot lower level to make sure they are in compliance.

[*Translation*]

Ms. Annick Papillon: Indeed.

Of course, we always assume that businesses will act in good faith and be diligent. However, we are here to draft a bill, and a lot of time has gone by before it was referred to the committee.

The matters raised here were also raised at the Senate as well as in previous Parliaments. That is why it is important that we draft a "2.0 bill", that is to say a very current, very modern piece of legislation. We fear there may be some gaps in this regard.

I would like to ask the other witnesses if they think businesses would be concerned about potentially contravening the law, while assuming of course at the outset that everyone is going to act in good faith. We have to ensure that businesses are diligent and see whether this act might generate some fear. This is the right time and place to speak out on the matter.

Mr. Brown, Ms. Romanko and Ms. Cooper, would you like to speak to this?

[*English*]

Mr. Douglas Brown: In the section that I commented on, clause 10, proposed paragraph (d.3), one of the protections in the reporting is that it's reported to a government institution, and as I said in my comments, the institution itself as it becomes defined is presumably going to have limitations on its jurisdiction and what it can do with the information. So in protecting the flow of information, at least for the sections I've commented on, that's probably a check and balance that's already built into the legislation.

[*Translation*]

Ms. Annick Papillon: That is indeed the case. Moreover, the importance of adequate resources has been raised several times, and not only by the Privacy Commissioner. This is the essential point that is being made at this meeting, I would say.

When greater powers are granted, there must also be additional resources. We say that we have to move forward, but this means additional human and financial resources. We have to be able to ensure that they will be there, otherwise, in practice, we will be far from being able to meet the objectives. That is obvious. In my opinion, that is the point that needs to be retained.

Thank you.

[*English*]

The Chair: Thanks, Ms. Papillon.

Now, Mr. Lake, you're the final questioner.

Hon. Mike Lake: Thank you again, Mr. Chair.

I don't think I'll need very much time. I wanted to follow up with Ms. Romanko. There was a conversation around clause 5 regarding section 6, the consent clause, and you made a comment a couple of people ago, which I believe had something to do with folks with the mental capacity to understand. Would you reiterate the point you were making there?

Ms. Catherine Romanko: Yes, the issue was about consent and the effect of providing consent to disclosure of information. I was simply making a point that an individual who is deemed at law to be mentally incapable is not able to provide valid legal consent for anything. That would apply also to a minor. In British Columbia the age of majority is 19. Anyone under the age of 19 cannot provide consent except in certain statutory exceptions. For example, they might be able to provide consent to treatment if they meet the mature minor test for medical treatment, but they would not be able to enter into a contractual relationship, for example, without intervention of the court.

There are other provisions to protect. The idea of consent by someone who doesn't have capacity at law to provide it was my point.

● (1245)

Hon. Mike Lake: All right.

Mr. Chair, I don't actually have more. I could fill time. I could talk for six minutes, but I don't think I have any more to add to that.

The Chair: Thank you very much.

We have another committee coming in, but we have three or four minutes if someone wants to make a final point—one of our witnesses. I'd be glad to hear it before the committee.

Mr. Levin.

Prof. Avner Levin: Just briefly, I haven't been asked questions about it, but I would like the committee to consider that point about the workplace privacy that I raised in my opening remarks, about making what I consider to be a very small yet significant amendment to that relative provision. I don't think it was the government's intention, as far as I understand it, to do away with the standard of having employers be reasonable, and I worry that the language as currently written is actually going to erode that in an unintended way. If the committee is going to consider some amendments, that is one thing, at least in terms of my addition to the conversation today, I'd very much like it to do.

Thank you very much.

The Chair: Thank you.

Ms. Cooper.

Ms. Janet Cooper: A couple of committee members asked about work product, and I want to just be clear that what we're talking about is de-identified data. It does not have any direct patient information on it, and the research that is done goes through ethics approval, very structured research. It is important not to just collect prescription utilization data but other health data as well to inform policy-making and that type of thing. It is certainly de-identified and it goes through very rigorous ethics boards.

The Chair: Thank you.

Mr. Brown.

Mr. Douglas Brown: I have nothing further.

The Chair: Ms. Romanko.

Ms. Catherine Romanko: I have nothing further.

The Chair: All right, thank you very much.

Colleagues, we have a robust meeting on Thursday with many witnesses, and we'll see you then.

We are adjourned.