House of Commons
CANADA

Standing Committee on Justice and Human Rights

JUST • NUMBER 034 • 2nd SESSION • 40th PARLIAMENT

EVIDENCE

Monday, September 28, 2009

Chair

Mr. Ed Fast

Standing Committee on Justice and Human Rights

Monday, September 28, 2009

● (1530)

[*English*]

The Chair (Mr. Ed Fast (Abbotsford, CPC)): I call the meeting to order.

Welcome, everyone, to the 34th meeting of the Standing Committee on Justice and Human Rights. Today is Monday, September 28, 2009.

You have before you the agenda for today. You will have noticed that today we are continuing our review of Bill S-4, An Act to amend the Criminal Code (identity theft and related misconduct).

We have before us four organizations.

Just so you know, one organization cancelled. The Canadian Association of Chiefs of Police had to bow out at the last minute. That leaves us with four organizations.

First, representing the Information Technology Association of Canada, we have Bernard A. Courtois.

We also have the Office of the Privacy Commissioner of Canada. Jennifer Stoddart is the commissioner, and Carman Baggaley is the strategic policy adviser.

Representing the Canadian Bar Association, we have Gaylene Shellenberg, who is a lawyer with that organization, and also Daniel MacRury, who is the treasurer.

Finally, we have the RCMP represented. We have Chief Superintendent Stephen White and also Inspector Kerry Petryshyn.

Welcome to all of you. I think you've been told the process. Each organization has 10 minutes to present. Then we'll open the floor to questions from our members.

Mr. Courtois, please proceed. You have 10 minutes.

[*Translation*]

Mr. Bernard Courtois (President and Chief Executive Officer, Information Technology Association of Canada): Thank you, Mr. Chair.

As you mentioned, my name is Bernard Courtois. I am the President and CEO of the Information Technology Association of Canada, the national association of the information technology and communications industry. We are very interested in seeing our economy develop into a digital, Internet economy.

[*English*]

We've been working for quite a while on all the issues around how Canada should make sure that it secures its place for success in the way that the global economy is going, becoming an Internet economy and a digital economy. We participated, along with many other people around our industry and others, in a big forum last June on trying to set an agenda for leadership in the digital economy for Canada.

There have been numerous gatherings around this issue. Every time we get people to look at this, the whole issue of confidence in the Internet and the digital economy as an economic instrument is front and centre. Confidence means that users have to have a sense that our laws are adapted to reflect these new realities, including the new threats that have come about because of the misuse of technology.

There is no doubt that for quite some time the whole issue of identity theft and identity fraud has been identified as a very important danger to protect Canadians against. Therefore, we welcome this bill and the approach it takes to tackle this problem. This includes a number of aspects: an open-ended list of what may be involved in identity documents and so forth, along with the possibility of reviewing the bill in five years. This is an area that moves so fast, we will want to live through this experience and see whether any adjustments should be made, particularly in the area of reasonable inference and whether that is enough to really capture and catch the behaviour that we want to catch, or whether at some point the capturing of someone else's identity information is, in and of itself, a sufficient inference.

On the whole, what we're here to do is to say that our association, which represents the industry most intimately involved with creating the Internet or bringing it to Canadians and the technology that makes it work, views this bill as an important element. We are quite supportive of getting it passed as soon as possible.

Those are my introductory comments. Thank you.

● (1535)

The Chair: Thank you very much.

Ms. Stoddart, you have 10 minutes.

Ms. Jennifer Stoddart (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): Thank you very much, Mr. Chairman. I don't think I'll take 10 minutes.

I have appeared on this question several times in the past few years. I've been fairly outspoken about the problem. I'm very pleased to see that the government is taking action on it today.

Polling conducted by my office this year has revealed that one in six Canadians has experienced some form of identity theft. Over 90% of Canadians are concerned about this issue of identify theft.

As you know, identify theft is a broad term that is often used to describe a wide range of behaviour. It can include credit card fraud, it often involves pretexting—pretending to be someone else in order to purchase goods or services or obtain that person's personal information. There are also more sophisticated techniques such as skimming, which involves stealing personal information from the magnetic strips of debit and credit cards through the use of small electronic devices.

I'm sure everyone here has received numerous phishing e-mails from what appear to be reputable organizations such as banks and caisses populaires—even the Government of Canada was a victim of phishing last year—asking us to verify our account information or provide personal information to the sender.

As technology evolves, identity thieves are constantly looking for new ways to obtain personal information. Just last month a man who has been called the world's most prolific identity thief pleaded guilty in Florida to stealing tens of millions of credit and debit card records by identifying and exploiting weaknesses in retailers' wireless networks.

[*Translation*]

Identity thieves then use this personal information to withdraw money from bank accounts, obtain loans or credit cards, obtain government benefits and even take out mortgages.

We often talk about identity theft in terms of the financial cost and while victims of identity theft may suffer significant financial loss, they are also likely to feel that their privacy has been invaded.

The lessons of the past few years teach us that stronger protections are needed if privacy is to have any meaning at all in the face of contemporary challenges. Bill S-4 is a significant step in the right direction. However, it should form part of a broader-based strategy to address identity theft and identity fraud.

The recent introduction of anti-spam legislation is also an important contribution to this process. The proposed Electronic Commerce Protection Act prohibits the sending of unsolicited commercial electronic messages without consent. It includes targeted provisions against phishing and spyware, and it provides a private right of action against spammers. The Act also sets out a coordinated approach to enforcement that allows for co-operation and information sharing with foreign authorities.

● (1540)

[*English*]

So that's another piece of legislation that is already before this House.

I would like to see a similar coordinated approach to ID theft. We have the expertise and the resources. There is the PhoneBusters anti-fraud call centre operated by the RCMP, the Competition Bureau, and the Ontario Provincial Police. There are excellent resources on identity theft on the Safe Canada website set up by Public Safety Canada. Now we really need the police and regulators, the public and private sectors, and federal and provincial officials to work together.

In our recommendations for the reform of the Privacy Act we have asked for stronger regulation, including better security safeguards, and we continue to believe that broader access to the courts is important for Canadians. In the review of our private sector legislation, PIPEDA, we have similarly recommended changes that would allow us to better regulate personal information handling practices, and we have called for mandatory breach notification for the private sector. These measures would empower Canadians to prevent identity theft and motivate companies and government organizations to properly safeguard personal information under their control.

Thank you once again, Mr. Chairman, for inviting me to speak on this very important issue. I will answer any questions as best I can.

The Chair: Thank you very much.

Who will be speaking for the Canadian Bar Association?

Ms. Gaylene Schellenberg (Lawyer, Legislation and Law Reform Directorate, Canadian Bar Association): I'll begin and Dan will take over.

The Chair: Ms. Schellenberg, you have 10 minutes.

Ms. Gaylene Schellenberg: Thank you for the invitation to present the Canadian Bar Association's views on Bill S-4 to you today.

The CBA is a national association of over 37,000 members, including lawyers, notaries, law students, and academics. An important aspect of our mandate is seeking improvement in the law and the administration of justice, and it's from that perspective that we appear before you today.

With me is Dan MacRury, the current treasurer of our national criminal justice section. The section represents a balance of crowns and defence lawyers from every part of the country. Dan is a prosecutor from Sydney, Nova Scotia. I'll turn it over to him to present the substance of our submission to you.

Mr. Daniel MacRury (Treasurer, National Criminal Justice Section, Canadian Bar Association): Thank you, Mr. Chairman.

I would like to thank the honourable members for the opportunity to make a submission today on behalf of the Canadian Bar Association criminal justice section.

The Canadian Bar Association criminal justice section commends the efforts of Bill S-4 to address identity theft and related criminal activity, as these are serious problems giving rise to significant individual and societal losses. We appreciate that Bill S-4 would restrict the scope of some of the proposed new offences so as not to inadvertently capture unrelated or innocent conduct, particularly in relation to new offences concerning identity documents and information. We also support Bill S-4's proposed removal of certain reverse onus provisions of the Criminal Code. We recommend several amendments that we believe add clarity and certainty to the proposals contained in Bill S-4.

The CBA criminal justice section's comments today are guided by three principles. One is the principle of legislative restraint. Revisions to the Criminal Code should only be made where existing provisions are inadequate. Two, any new proposals must comply with the Charter of Rights and Freedoms. Three, changes to the Criminal Code alone are generally insufficient to address serious or complex problems. To be effective, such changes must be accompanied by refinements in law enforcement practice and procedure, increased public education, or other legislative amendments.

The last observation may be particularly applicable to the problem of identity theft. The federal Privacy Commissioner and other organizations have noted that an effective response to identity theft will require a comprehensive approach, including a broad range of initiatives in addition to changes to the Criminal Code. In other words, there has to be more than one tool in the toolbox to address this serious problem.

We would like to make the following recommendations. First, Bill S-4 should be amended to expressly exclude the general provisions of attempt and counselling and certain types of *de minimis* behaviour.

Second, the relationship between the new offences proposed in Bill S-4 and the existing general provisions should be clarified.

Third, the proposal to prohibit possession of identity information should be amended to offer greater clarity by replacing the term "is reckless" with more explicit language.

Fourth, the exemption for certain police activities in clauses 7 and 9 of Bill S-4 should be removed.

In relation to recommendations one and two, the bill defines a new category of documents described as identity documents. It proposes a wide range of offences, including procurement, possessing, and selling social insurance numbers, drivers licences, etc. Given the combined scope of the definition and the proposed offences, we believe that the bill's proposal to add new defences to the existing concept of lawful excuse is appropriate. It is a clear attempt to restrict the reach of these provisions and is consistent with the concerns we have addressed in the past.

In spite of Bill S-4's proposed restrictions, other jurisdictions go further to restrict the reach of similar provisions in two ways. First, they expressly exclude the general provisions of attempt and counselling. Second, they expressly exclude certain types of *de minimis* behaviour, such as for young persons possessing identity documents to gain admission to licensed premises.

The criminal justice section recommends that Bill S-4 be amended to expressly exclude general provisions of attempt and counselling and certain *de minimis* behaviour. There also should be some clarity between the existing provisions and the new bill.

On our third recommendation, the section believes that the term "reckless" should be clarified. Proposed section 402.2 prohibits possession for the purpose of transmission, making available, distribution and sale, or offer for sale of that information where an individual knows, believes, or is reckless as to whether the information will be used to commit an indictable offence containing an essential element of fraud, deceit, or falsehood.

Including recklessness as a form of the mental element for this offence could be seen as responding to the Supreme Court of Canada in R. v. Hamilton. We also note concerns about the formulation, particularly as it might apply to businesses or industries that handle large volumes of such information. While the term "reckless" is used in the Criminal Code, it is not free from controversy and occasional interpretive difficulty.

● (1545)

To provide greater clarity and to address some of the business and industry concerns, we suggest more explicit language. For example, in R. v. Hamilton, the Supreme Court of Canada equated recklessness with "conscious disregard of the substantial and unjustified risk".

In the Hamilton decision, the Supreme Court of Canada, at paragraph 28, stated:

> The "substantial and unjustified risk" standard of recklessness has venerable roots in Canada and in other common law jurisdictions

It cited cases, and then the court went on to say:

> Finally, a brief word on *R. v. Sansregret*.... The Court in that case defined recklessness as the conduct of "one who, aware that there is danger that his conduct could bring about the result prohibited by the criminal law, nevertheless persists, despite the risk...in other words, the conduct of one who sees the risk and who takes the chance".... The Court, in *Sansregret*, did not set out the degree of risk required to attract criminal sanction.

As well, in the decision, the Supreme Court of Canada said at paragraph 33:

> We have not been invited in this case to revisit *Sansregret* or to consider afresh the governing principles of recklessness

It is our submission today that, without clarity in the definition, the courts will have to consider afresh the governing principles of recklessness.

That deals with our concern in relation to recklessness.

Our fourth recommendation to you today deals with the exceptions for police and other official acts. Clauses 7 and 9 propose another exemption for certain activities for public officers as defined by section 25.1 of the Criminal Code. Given the existing legislative scheme, it is unclear why another exemption might be necessary. The Canadian Bar Association criminal section has strongly opposed an exemption from criminal liability for police or their agents, arguing that the law should apply to everyone, but acknowledges that the existing sections contain certain detailed procedural safeguards and reporting requirements. We see no reason the acts specified in Bill S-4 would be inadequately addressed by the existing scheme, and we are opposed to creating further exemptions of this sort.

The criminal justice section recommends that the police activities in clauses 7 and 9 of Bill S-4 be removed.

In conclusion, this section recognizes the prevalence and seriousness of identity theft. We appreciate the efforts in Bill S-4 to provide narrowly circumscribed new offences to address the issue without inadvertently capturing what should properly be non-criminal activity. To further advance this objective, we suggest some clarity in the language of the bill—for example, surrounding the mental element of recklessness, as well as a clarification of the interaction between some of the proposed offences and the attempt and counselling provisions of the code. We also appreciate the proposal to increase the use of a hybrid structure of offences to give greater flexibility and scope to prosecutorial discretion in dealing with these matters.

I would like to thank the honourable members for this opportunity this afternoon.

● (1550)

The Chair: Thank you very much.

We'll move on to the RCMP. Superintendent Stephen White, you have ten minutes.

Chief Superintendent Stephen White (Director General, Financial Crime, Royal Canadian Mounted Police): Thank you.

Good afternoon, Mr. Chair and honourable members of the committee. Thank you very much for inviting us to be a part of today's hearing. Here with me is Inspector Kerry Petryshyn, officer in charge of major fraud and bankruptcy within our commercial crime branch.

I appreciate having this opportunity to present the RCMP's perspective on the current state of identity theft and fraud in Canada.

White collar crimes come in many different forms, including mass marketing fraud, payment card fraud, identity theft and identity fraud, capital markets fraud, and money laundering, as a few examples. The significant growth of technology and the widespread use of computers have led to great advances in research and global communications, but they've also opened the floodgates for enterprising criminals. Technology has had a significant impact on the manner in which economic crimes are committed, their frequency, and the challenges faced by investigators dealing with this type of crime.

As businesses and financial transactions become more and more Internet dependent, new opportunities are emerging to facilitate financial crimes. Before computers and the widespread use of the Internet and other associated technology, stealing and using another person's identity was a relatively difficult crime to commit. Criminals had to invest considerable time and effort in the process, and the risks were high. To assume someone's identity, a thief had to break into a house, or steal a purse or a wallet. Today's technologically adept thieves can do just as much damage in the time it takes to swipe your bank card through the reader at a cash register.

The same technology that has made our lives more convenient by allowing us to shop from home and operate in a virtually cash-free marketplace has also given rise to countless new criminal opportunities for identity thieves.

[*Translation*]

They can now steal your personal information from the comfort of their home offices half a world away, taking advantage of everyday transactions that require people to share personal information for identification purposes.

[*English*]

The growing impact of identity theft and fraud is deeply troubling. A 2008 EKOS survey found that 9 out of 10 Canadians were somewhat concerned that they could be victimized by identity theft and fraud. The survey also indicated that Canadians ranked the economic crimes of fraud and identity theft as their number one concern, more troubling than terrorism, organized crime, and gang violence.

That's why we have to view economic crime as being every bit as serious as many other types of criminal activity. It is true that identity theft and fraud, for example, are less physically dangerous than many types of criminal activity; however, their social damage can be very severe and can undermine the trust that people have in their society.

[*Translation*]

The cost to a person who has had his or her identity stolen can be enormous: financial loss and the investment of hundreds of hours trying to re-establish identity and good credit all take their toll.

[*English*]

A recent study by McMaster University estimated that in 2008 1.7 million Canadian identity theft victims spent 20 million hours and $150 million clearing their names. Of course, individuals aren't the only victims. Stolen identities are also used to commit frauds involving government services, benefits, and official documents. Financial institutions and retailers, the foundation of our economy, suffer growing losses every year.

Evidence indicates that identity fraud isn't just committed by enterprising individuals. Organized criminal groups are also applying their considerable resources to this expanding field of opportunities.

Quantifying the damage is extremely difficult. Many instances of this type of fraud go unreported, so definitive statistics are hard to come by. PhoneBusters, the Canadian Anti-Fraud Call Centre jointly operated by the RCMP, the Ontario Provincial Police, and the Competition Bureau of Canada, can only maintain statistics on the complaints they receive. In other words, the more than 11,000 complaints received by the call centre in 2008 reflect only a small percentage of the problem.

The Canadian Council of Better Business Bureaus indicated that identity theft was the fastest growing type of fraud in North America, with the cost to consumers, banks, credit card firms, and retailers estimated to be in the billions of dollars each year.

Raising public awareness about protecting personal information is currently the best tool we have for preventing identity fraud. Along with members working in RCMP detachments across the country, members in our financial crime units make numerous presentations to educate the public on this issue.

Whether these presentations are made to businesses, government agencies, or community groups, the messages are the same: protect your personal information, shred unwanted personal documents, and be wary of suspicious e-mails. Prevention is still the best cure, but prevention can only do so much.

Identity fraud is clearly emerging as an immense problem. In consultation with key stakeholders and other law enforcement agencies, the RCMP is developing an identity fraud strategy focusing on criminal intelligence and analysis, prevention through education and awareness, and disruption and enforcement.

● (1555)

[*Translation*]

We are also heading up the creation of an international identity fraud working group, the objective of which is to obtain an overview of other countries' identity fraud strategies, discuss related joint priorities, and develop an international strategy.

[*English*]

Currently the Criminal Code does not contain specific offences pertaining to identity theft. Most Criminal Code offences relating to property crimes were enacted before computers and the Internet were even invented. While the Criminal Code addresses most fraudulent uses of personal information by identity thieves, it does not address the unauthorized collection, possession, and trafficking of personal information for the purpose of future criminal activity.

As I indicated in my opening remarks, the changing environment is one of the greatest challenges we face in our efforts to combat financial crime. The growing sophistication of this type of criminal activity is abetted by the same techniques and technologies that spur legitimate opportunities for business.

Why be reactive when we can be proactive? We must be constantly examining our environment to identify new tools that can greatly assist us in investigating white collar crime.

Bill S-4 will close legislative gaps that currently allow criminals to collect, possess, and traffic in personal identification information and documents. Legislative amendments aimed at closing the identity theft gap would help the RCMP and other law enforcement agencies protect not only individual Canadians but also the integrity of our economy. We welcome laws that will move us closer to this goal.

Mr. Chair and honourable members of this committee, that concludes my prepared remarks. Now we will be happy to answer any questions you may have.

Thank you.

The Chair: Thank you very much to all of you.

We will open the floor to questions, beginning with Mr. LeBlanc for seven minutes.

Hon. Dominic LeBlanc (Beauséjour, Lib.): Thank you, Mr. Chairman.

[*Translation*]

Ladies and gentlemen, thank you all for your presentations.

As Ms. Stoddart noted, Parliament has been concerned about this issue for some time now, and with good reason. I think we have come to the point where we need to move fairly quickly to adopt this bill. I hope that we can work with colleagues to make that happen as soon as possible.

[*English*]

I want to ask Mr. MacRury a question about his comments and then perhaps Chief Superintendent Stephen White.

Mr. MacRury, at the beginning of your comments you said that Criminal Code amendments or changes to criminal legislation represented one tool amongst many others to deal with what is obviously a growing and serious problem with economic crime, white collar crime, and in this particular case, identity theft. What other tools would you advocate?

I know I am getting you off your script, and I may ask you about a specific amendment you suggested, but I was curious when you began by saying that it's one tool. What other tools do you think Parliament or the government could give police forces or prosecutors to clamp down on what is a growing problem?

Mr. Daniel MacRury: It is obviously in our presentation, but thank you for the question.

Obviously what was mentioned by the RCMP, which is an international strategy, is very important. I've had the opportunity of prosecuting cybercrime cases, and we might as well face the reality that these have no boundaries. So having more of an international strategy, I believe, is certainly one aspect that has to come about as well.

Also, for example, the training of police and prosecutors in this area is always important. As indicated by the others who have testified today, this is an ever-changing area. So it's important to keep up-to-date and to keep ahead of the curve.

For example, in my province, I had the opportunity of being trained about cybercrime at the district attorney school in South Carolina. Then through the auspices of Justice Canada, they trained prosecutors across the country on cybercrime.

So these types of strategies, I would submit, are certainly important. Education and prevention are important.

As somebody who has practised criminal law for over 20 years, I can personally say that we can deal with deterrence and everything else, but unfortunately, when it gets to our stage, the damage has been done. So we need to help people by educating them to watch out for these perpetrators. I think education is a very important aspect to protect Canadians.

Certainly, whatever enhancement and cooperation we can get from all sectors, as Ms. Stoddart said, is crucial.

● (1600)

Hon. Dominic LeBlanc: So your point is that investments in prevention and education for those in the criminal justice system are equally important elements in fighting identity theft. It's not simply a matter of changing the Criminal Code that will solve the problem.

Did I understand you correctly?

Mr. Daniel MacRury: That's correct. In other words, we want to be able to cut the market off so that people don't get duped by these things. All you have to have is one victim before you. You realize, yes, you will get a conviction, and yes, you will get a sentence, but there's no doubt that their confidence in the system has been shaken.

Hon. Dominic LeBlanc: Mr. MacRury, again, you perhaps referred to this in your comments with respect to recklessness, or maybe I inferred some element of a criminal intent, but you referred to an all-too-common example that we probably all see in our constituencies, and sometimes even in our own families, of the 18-year-old kid who wants to go out with his 19-year-old buddies to a pub and who has an ID card that may not be his own and who shows it a doorman to be able to go into the pub with his buddies. How would this provision apply to that circumstance, if it would apply at all?

Mr. Daniel MacRury: Well, I think it's wide enough that the legislation may apply, and that's our concern. I think this situation should specifically be excluded so it doesn't apply. This is a good piece of legislation, and you don't want someone using it too broadly and making the mistake of prosecuting somebody for that, when we have more serious individuals to go after. I guess that's our concern. Other jurisdictions have been more explicit in excluding that. I think it's important. It's in recommendations 1 and 2 in our brief.

Hon. Dominic LeBlanc: Thank you.

Mr. Chairman, do I have any more time at all?

The Chair: Yes, you do. You have just under two minutes.

Hon. Dominic LeBlanc: Thank you, Mr. Chairman.

This is a brief question, perhaps to Chief Superintendent White. What we've learned at this committee and what we've learned in conversations across the country is that police forces across the country—the RCMP obviously being the biggest one—are wrestling with the very difficult context of economic crime. We've seen in Quebec examples of white collar crime that have shaken confidence in whole sectors of the economy. We've seen it across the country. It's not only in Quebec, but it has achieved a lot of media attention there.

One thing we've heard, Chief Superintendent, is that again, Criminal Code amendments are part of the solution—tough sentencing, making it impossible to receive accelerated parole, for example. These are all things we would support. But our sense from police officers is that that alone is not enough. The police forces are asking for more resources and more tools, whether it's amending the Criminal Code with respect to electronic surveillance or modernizing some of the technology that police can access.

I'm wondering if you could very briefly tell us what other suggestions you have for this committee or for Parliament in terms of making your life easier in catching these criminals, hopefully before, as Mr. MacRury said, much damage is done.

● (1605)

C/Supt Stephen White: Thank you very much.

Obviously the broader spectrum of white collar crime would bring into play a lot greater tools than the issue before us today with regards to identify theft, identify fraud. I think one of the big issues, and Mr. MacRury mentioned it, is how we can take a more comprehensive collective approach, specifically with regards to issues like identify theft and identify fraud, but even broader, expanding that out to issues like mass marketing fraud, which is still a huge problem here in Canada today and internationally. That comes down to a collective effort, especially with regards to the collection of intelligence information, the analysis of that.

Actually, if we could do a good job at that, it should lead us on two spectrums. One, the more information intelligence we can gather collectively from across the country from all law enforcement agencies and bring that together into a national central hub where we can analyze it.... Because a lot of this activity that's taken place, whether it be identify theft, identity fraud, or mass marketing fraud, is taking place from outside of Canada. None of the victims are centred in any one particular area in Canada. The whole success of people involved in this type of activity is that they target a broad scope of victims across a broad geographic area, basically right across the country.

Individually, in a lot of jurisdictions, two or three small complaints with regards to identify theft, identify fraud, for example, may not mean a whole lot to local police jurisdictions if they're prioritizing their investigations. However, if we collect that all together nationally, that's where we start to identify and see a big picture. Getting that national picture helps us to identify the large organizations that are involved in this type of activity. The stats clearly indicate that if we have millions of victims here in Canada, law enforcement will not be able to investigate all those individual complaints. The best approach I think we can take is to collectively get as much information as we can, identify the emerging issues that are coming forward with regards to identify theft and identify fraud. If we can identify them as they're emerging, then we could do a much better job in terms of awareness, education, and prevention, which should be, for all of us collectively, our ultimate goal. At the same time, if we can identify the large organizations that are involved in this and impacting Canadians, that's where we can focus and prioritize our resources.

The Chair: I'm going to have to stop you there. Thank you.

I'm just going to remind our witnesses to try to keep your answers as brief as possible. Thanks.

We'll move on to Monsieur Ménard. You have seven minutes.

[*Translation*]

Mr. Serge Ménard (Marc-Aurèle-Fortin, BQ): Thank you, Mr. Chair.

First of all, I want you all to know that I am somewhat disappointed. This is the first meeting of this committee that I have attended. In the case of the other committees, I always liked to read the witnesses' submissions before the meeting, in order to be able to ask more relevant and intelligent questions. I only received one submission in advance of this meeting, and only when I arrived here at that. That was the brief of the Canadian Bar Association. I had tremendous faith in the witnesses that they would tell us whether or not they agreed with this proposed legislation which, in our opinion, seemed necessary a priori, but initially, difficult to develop.

You can correct me if I am wrong, but as I understand it, Ms. Stoddart, the Office of the Privacy Commissioner is more or less completely satisfied with the proposed legislation. The Canadian Bar Association has suggested a few changes to us, but it is very difficult to follow along without a written text. It's so much easier with one. I also understand that law enforcement agencies are more or less prepared for this legislation.

I would like to ask a question that has long concerned me and I would appreciate a succinct answer. Twelve numbers appear on the back of our credit cards. What is the purpose of the last three digits on the back of the card that are not embossed? I used to think they had something to do with security, that basically, they were tied in some way to our relationship with the individual... People have asked me if they are required to give out these last three digits over the Internet when requested to do so.

Perhaps Mr. Courtois, an industry representative, could enlighten us.

Mr. Bernard Courtois: The credit card system is not my particular area of expertise, but I do know that there are additional levels of security and verification. In some case, people are asked to give out only the numbers appearing on the back of the card. Occasionally, they are asked to provide the last three digits on the back of the card. In the case of somewhat more delicate transactions, the cardholder may be asked to provide some personal information that he or she shared with the financial institution when applying for the card.

These are merely additional layers of security that the person you are dealing with is relying on.

● (1610)

Mr. Serge Ménard: The next time, I won't give out these numbers. Then I'll see what type of questions I'm asked.

I have a question for the RCMP. These challenges have made you realize, as others have, that a modern police force requires considerable expertise, particular in the area of information technology. Although universities sometime offer IT courses, we have discovered that people are often self-taught and that it is these individuals who are the most adept at hacking into systems.

Briefly, how many RCMP officers are experts in information technology, and what kind of training do they have?

[*English*]

C/Supt Stephen White: Unfortunately, I'm not in a position to give you a specific figure in terms of the number of experts we have in informatics and technological-crime-type issues.

What I can say is that we have a well-established technological crime unit within the RCMP. We have a very significant informatics component to our national organization. They have significant numbers in them. I don't have the exact numbers for you here today, but I would be happy to get you those numbers.

[*Translation*]

Mr. Serge Ménard: I would be very happy if you would follow up on this for me. I'm not asking you to reveal any confidential information. RCMP operations will not be affected. I would greatly appreciate it if you could let me know how many people are employed in your largest unit and in your specialized informatics unit.

I would like to read the Canadian Bar Association's submission. However, as I recall, the changes that you are proposing are few and relatively minor. Basically, as I understand it, you, the experts, are satisfied with the proposed legislation and believe that we should move to adopt it as quickly as possible. Is that right?

I have one final comment. Back in 2000, I was struck by a television program that I saw. It showed the CBC interviewing some people back in 1950. They were asked to give their predictions for the year 2000. Many predicted that people would be travelling to the moon and into space. They predicted honeymoons spent in zero gravity conditions, video phones and all kinds of things. A lieutenant in the French navy was also interviewed. I really don't know why he was, but he gave the best prediction of all. He predicted that computers would transform our lives by the year 2000. He was spot on with his prediction.

I still bragged about being computer illiterate in 1996. Since then, I have made an effort to improve my skills and I will admit that I couldn't do without my computer today. However, I do get the impression that some of the information that I transmit via my computer could become public knowledge. My banking transactions are conducted strictly with my bank. I feel that if I start to transfer sums of money from one bank to another, I could be a victim of theft. Am I cautious enough? I agree that it's a marvellous tool for paying bills. So far, I have not had any unpleasant experiences. However, I think that if I were to start transferring funds from one bank to another, then I would be putting myself at risk. I've just read an excellent novel by the name of *Millénium* that deals with this very subject. Has anyone else read it?

● (1615)

[*English*]

The Chair: Monsieur Ménard, you're out of time. Thank you.

To be fair to our witnesses, I have checked with the clerk, and it is our common practice to let them know that they can present a brief in advance, but it's certainly not compulsory.

As you know, Monsieur Ménard, many of our witnesses appear here on relatively short notice. Any briefs that have to be circulated also have to be in both official languages, and sometimes that becomes very difficult.

We'll move on to Mr. Comartin, for seven minutes.

Mr. Joe Comartin (Windsor—Tecumseh, NDP): Thank you, Mr. Chair.

I'd like to thank you all for being here.

Mr. MacRury, the point you raised with regard to clauses 7 and 9 is the same point that I had raised with the minister and the officials when they were here. The justification we got, particularly with regard to proposed section 368.2, was that they specifically wanted to exclude it from section 25 of the code because they would be using it so often. The paperwork of having to report it would become so difficult that they may in fact not use the technique, one of the tools.

I must admit that I didn't catch it at the time, but I wasn't sure, after I thought about the answers later—this was one of those bright thoughts you have after the fact rather than at the time—how they would know that in terms of how often they would use it. Superintendent White or Inspector Petryshyn, you might be able to make some comment on that. From your experience with prosecutions, perhaps, does that make sense?

Finally, on the same point, Ms. Stoddart, again I think I missed the significance of what's in clause 7. It's not just police forces who would be asking this; it's also the Canadian Forces, along with the department or agency of a federal or provincial government. Any one of those agencies can now ask for a forged document, in effect, to be created. I'm just wondering if you would have any concerns about the potential for abuse there, given that you have such a broad scope of agencies who might in fact be asking for that.

Mr. MacRury, perhaps I can start with you, please.

Mr. Daniel MacRury: Of course, one is that the CBA's position is very clear that it shouldn't be changed. That's still our position.

To answer your question in terms of the paperwork, from my personal perspective and experience I can tell you that whether it's more paperwork or not, the rule of law is very important. When you're making exceptions to the rule of law, quite frankly, more paperwork and those protections and safeguards in section 25 are essential. It may slow things down, but at the same time, you have to balance out why you're slowing it down. You're slowing it down because it's an exception. When you're dealing with exceptions you have to take exceptional measures. From my experience, an analogy, Mr. Comartin, is that part VIs and wiretaps are very lengthy. I've had the opportunity to deal with part VIs. But they're lengthy for a reason, because of what you're dealing with and the balancing of rights. That's why the CBA position is quite clear that this exemption is not needed; the law shouldn't change.

Mr. Joe Comartin: Superintendent White, the impression we were left with by the minister and the officials is that it was going to be used quite extensively. I don't want you to put yourself in their shoes, but have the RCMP done any analysis of how often clause 9 in particular would be used, the proposed section 368.2?

C/Supt Stephen White: I'm not sure we've actually done any analysis and I don't think I'm in a position to say exactly how many times it gets used. I think what I can say is that it would be used on an extremely regular basis. I think the use of identification by undercover officers is actually the foundation of having an undercover program—being able to use on a daily basis covert identification. Undercover operations take place extremely often in a very fast and robust fashion, with short timeframes, on a daily basis. I think the way we would look at it is that this is a tool that our undercover officers would use like many other law enforcement tools that they have in their possession. It would be a daily tool as opposed to section 25.1, which is crafted for when police officers are going to take part in a specific criminal activity with regards to an ongoing specific investigation. I think that's the big difference, and that's why we would be strong supporters of leaving the exemption in the act for law enforcement.

● (1620)

Mr. Joe Comartin: Let me tell you the problem I'm having with this.

I sat on the committee when we did the review of Public Safety and section 25 when it came up for its mandatory five-year review. We were told at that time very clearly that it had hardly ever been used. I think we had five reports a year. We're undercover now. So are police forces breaking the law now and not reporting it?

I'm having some real difficulty understanding how prevalent this is, because if it is so prevalent right now before this comes into effect, how come it's not being reported?

C/Supt Stephen White: The use of identification?

Mr. Joe Comartin: Under section 25, why is it not being reported?

C/Supt Stephen White: Because it is not being used to facilitate a criminal activity; it's being used for the purpose of law enforcement investigations, the use of identification by an undercover police officer.

Mr. Joe Comartin: And that does not extend into criminal activity?

C/Supt Stephen White: There's nothing that prevents us from using it as a piece of identification, as a tool for law enforcement to pursue criminal investigation.

Mr. Joe Comartin: Ms. Stoddart, on clause 7.

Ms. Jennifer Stoddart: Very briefly, I don't have problems with clause 7. I'm not a criminal lawyer, but this opinion is based on a few things.

One is that in the years in which I've been Privacy Commissioner I have been continually amazed by the sophistication of the privacy breaches that we see. There are links to organized crime, to international organizations, and the difficulty for all our societies to come to grips with them. We've been involved in one of these international cases ourselves, and so on.

Secondly, I read that this paragraph is limited to those who act in good faith, which seems to me to put an important qualifier on it.

Thirdly, my understanding is that in many areas of the law it is necessary to use, let's say, forged documents, or what others say are forged documents, in order to set up a situation to prove a misdemeanour or an infraction of civil law. Certainly in the years I worked in human rights legislation it was a well-known fact that you could use testing to prove that, for example, certain types of housing are not rented to certain types of citizens, whether it be on the basis of their race or the fact that they have children, and so on. So it does not seem to me inherently offensive that we use to further the public good a document that was produced specially and would otherwise fall afoul of the other provisions of the act.

The Chair: Thank you.

We'll move on to Mr. Norlock, for seven minutes.

Mr. Rick Norlock (Northumberland—Quinte West, CPC): Thank you very much, Mr. Chair; and thank you to the witnesses for being here today.

I'm usually, and in this instance, particularly concerned about victims. They are the people who seem to be least considered when legislation is being formed. But in Bill S-4, as far as I'm concerned, the victim seems to be the primary concern, and that's a refreshing change.

This question is primarily for the RCMP, but Ms. Stoddart, please feel free to interject should you have something to add that you feel is pertinent.

What I particularly like about this bill is that it contains a provision where offenders will be required to pay restitution to the victims of identity theft and fraud when it comes to the costs of reclaiming their own identity. As I've mentioned, this is a welcome provision.

Having been recently a victim with one of my credit cards being cloned, I can say it didn't cost me anything directly, but we all have to be adult enough to know that when the credit card companies suffer a loss, guess who ends up paying for that loss: it is each and every one of us. So as we attempt to mine out these organizations, these criminal enterprises, and go after them, I believe this is a welcome provision.

By the way, I recently saw some numbers on the cost of identity theft, and I think it was conservatively estimated, just for Canada alone, at about $2 billion a year. Again, because of its nature, we don't know, but $2 billion as a conservative estimate means it's probably closer to $4 million or $5 million, I suspect.

Chief Superintendent and Inspector, in your experience, what kinds of hardship will a person who is victimized by identity theft face, and how likely are they to recoup anything? I ask that not to be facetious or anything. I know much of it will be anecdotal, when you speak to members who are in the field, etc.

Perhaps Ms. Stoddart can then also comment from her perspective.

● (1625)

Inspector Kerry Petryshyn (Officer in Charge, Major Fraud and Bankruptcy, Commercial Crime Section, Royal Canadian Mounted Police): It certainly varies from victim to victim. As you said yourself, having a credit card compromised may not cost you specifically. I suppose it would depend on to what extent the data is being used. We have some criminal organizations that will use your data to develop an entire persona and, through that, get perhaps government services, bank loans, mortgages, etc. The greater the identity that has been duplicated from you, the greater the cost. So trying to re-establish your identity after it has been compromised to the point where you have 20 or 30 creditors calling you weekly to say you owe them a considerable amount of money can take a long time, sometimes two or three years. Beyond dollar value for cost, there can also be an emotional cost, with the pain and suffering and the grief for those two or three years.

Mr. Rick Norlock: In your experience has there been any attempt at restitution when there is an accused finally convicted? Obviously if someone has been defrauded out of millions of dollars, or even thousands of dollars, one would assume an ability. Is there an ability? Have you seen a way of tracking that money and then coming upon a bank account of the accused or that organization and the crown going after restitution so that at least the victim is somewhat compensated for the crime that has been perpetrated against them? Have you seen it personally or from any reports?

Insp Kerry Petryshyn: Certainly in some cases I have personally witnessed examples where restitution was asked for. But as you mentioned earlier, quite often it is the case that there simply isn't anything to obtain from the accused. Either the money has been consumed or passed on somewhere up the chain in the organization or hidden in an offshore bank account somewhere, never to be found again. Unfortunately, the victims themselves are left with problems, and the problem of being able to hire their own legal representation, if necessary, to try to pursue it civilly.

There have been a few cases. I will use a credit card example. Often the credit card company itself is the victim per se. Therefore, they are usually the first to receive any recouped funds, if there happen to be any. I've had a few cases where we did manage to recover some money, but the credit card companies reclaimed that first.

The Chair: Ms. Stoddart.

Ms. Jennifer Stoddart: Thank you for your questions, honourable member, I think they go to the heart of why I'm supporting this bill. We do see provisions, unusually—this is a growing trend in Canadian law—for compensation to the victim and not just to the crown.

The issue of damages in the work we do, which is not criminal work, as the RCMP have explained, does vary widely and depends on the harm. Some people may have misuse of their personal information, but it's very hard for them to prove what harm they suffered, even emotional harm in some cases. It's a very broad range. Usually, in our experience, in that case the organization that mishandled the personal information—remember we are dealing with privacy matters, not with criminal issues—will restitute the amount of the loss and usually a bit more in terms of a moral compensation to the victim once this is proved by our investigation process.

The issue you raised that all Canadians indirectly bear the costs of credit card fraud is one I'm very happy to see you raise. I have spoken about this very much in the past few years. I thought that I'd just add to your deliberations today.

I mentioned one of the world's greatest computer fraud artists who has just been convicted. He was involved in the data theft at TJX, which my office investigated with the Alberta commissioner's office two years ago. We were the first body in the world to make our investigations known. He has been charged in the United States with a 19-count indictment that includes conspiracy, wire fraud, and aggravated identity theft charges under an agreement with the prosecutors. This was in late August. He'll face a maximum of 25 years in prison and will forfeit more than $2.8 million in cash. Unlike in some of the other examples that Inspector Petryshyn gave us, it seems that he had quite a few assets that could be liquidated in order to restitute his victims.

● (1630)

The Chair: Thank you.

As the Liberals don't have any more questions, we'll move on to Madam Brunelle. You have five minutes.

[*Translation*]

Ms. Paule Brunelle (Trois-Rivières, BQ): Good day.

Ms. Stoddart, you said something that I found quite interesting, namely that victims of identity theft are likely to feel that their privacy has been invaded. How many times have we seen where people's homes are broken into and their concern is not for the material possessions they may have lost, but for the fact that their privacy has been invaded. This is a major worry, especially for seniors.

You claim that while Bill S-4 is a significant step, it should form part of a broader-based strategy to address identity theft and identity fraud. Briefly, what type of strategy do you foresee?

Ms. Jennifer Stoddart: Thank you for the question.

As other witnesses have noted, the Government of Canada and Canadian law enforcement agencies are cooperating to ensure that information is shared, not only within Canada but abroad as well, as quickly as possible. Judging from our experience, speed is a factor in this type of crime which increasingly depends on the fact that jurisdictions are divided. Deliberate efforts are made to change jurisdictions. The fact that Americans target Canadians as victims creates problems because it is difficult to prosecute people who are in the United States. The reverse is also true. That is one of the reasons why I have forged ties with the civilian Federal Trade Commission. I want assurances that it is possible to mount a common front to address these problems. This is just one example, but the fact remains that cooperation, public education and a concerted effort are all extremely important.

Ms. Paule Brunelle: What you are saying calls to mind another issue. When I was my party's industry critic, film theft was a problem. It would happen so quickly that the police did not even have time to respond. Films were recorded directly by people in movie theatres. In the blink of an eye, these films were sent abroad.

Isn't it true that these fraud artists are so malicious that it is impossible to intervene quickly enough and that with our legislation, the process is even more protracted?

Ms. Jennifer Stoddart: Law enforcement agencies may have always thought, based on their experiences, that criminals were one step ahead of them. Clearly the legislative process is out of step with the times, given the speed at which crimes can be committed today. The lack of cooperation and contemporary legislation creates ideal conditions for criminal activities.

Ms. Paule Brunelle: My next comment is directed to the RCMP spokesperson.

In your submission, you talk about how raising public awareness is a key factor. However, I wonder if that it really effective. Education and awareness happen over the long term. What, in your opinion, would truly discourage criminals from committing fraud? Does Bill S-4 really address the problem?

[*English*]

C/Supt Stephen White: I don't know if we'll ever be able to deter everyone from becoming involved in these types of criminal activities. In terms of deterrents, what we see in this bill as the big benefit is having offences that will at least enable us to have a greater impact in terms of those individuals who are acquiring, possessing, and trafficking personal identification information for the purpose of eventual additional fraudulent activity. What it will give us is a tool at the front end, which we really don't have now, and that will enable us to intercept and hopefully arrest, prosecute, and impact these organizations at an earlier stage, hopefully even before the fraudulent activity has actually taken place.

● (1635)

[*Translation*]

Ms. Paule Brunelle: When a person's credit card is cloned, credit unions and banks compensate the victim for any financial losses incurred. Are losses insured by the insurance companies? Aren't companies the ones putting the most pressure on police to resolve the problem? It must cost them quite a bit. A witness talked earlier about the significant costs this represents in Canada since victims of fraud receive a certain amount of compensation.

[*English*]

The Chair: Give a very quick answer, please.

C/Supt Stephen White: Yes. To my knowledge, it is the credit card companies or the banking institutions that cover the loss for credit card or debit card fraud.

The Chair: Thank you.

We'll move on to Mr. Rathgeber. You have five minutes.

Mr. Brent Rathgeber (Edmonton—St. Albert, CPC): Thank you very much, Mr. Chair.

Thanks to all the witnesses for your excellent presentations.

I want to pick up on a question for the Canadian Bar Association that my friend Mr. Comartin raised with respect to your objections to clauses 7 and 9. I thought I understood this, but I was confused by some of the dialogue.

In light of the law enforcement exemptions that currently exist in section 25 of the code, why specifically do you advocate that clauses 7 and 9 of Bill S-4 be removed?

Mr. Daniel MacRury: Because you have the exemptions and the procedural safeguards already in place in section 25. The Canadian Bar Association has been on record in the past not to support any more widening of this area. I think in the circumstances, given that you have section 25, it's not necessary.

Mr. Brent Rathgeber: I'll ask the same question to the RCMP.

I'm assuming you're going to take a different position, as do I, that clauses 7 and 9 do give you the protection you need.

C/Supt Stephen White: Yes, that is the protection we are looking for.

Again, our position is that we would prefer to have the exemption in this section rather than in section 25.1, for the same reasons as I mentioned earlier. The use of identification by undercover police officers is a tool they use on a daily ongoing basis; it's not a one-time tool such as pursuing a one-time criminal activity, for which we would seek justification under section 25.1. It's a tool they need. As I said earlier, the whole foundation of an undercover program is being able to use undercover identification. Because it is a daily tool that they require and use, we're looking to support it in its current fashion.

Mr. Brent Rathgeber: Thank you, Superintendent White.

In response to a question that you answered for my friend Mr. LeBlanc, and also for Ms. Brunelle, I think, regarding advancements in technology that white collar criminals and organized crime frequently employ, I think your response—and I don't mean to paraphrase you, because I know I'll do it inaccurately—was that law enforcement has a difficult time keeping up to the technological advancements that white collar criminals have access to, and that you're always a step behind, but this is one tool.

I was just wondering if you might be able to comment on this. I know you are not here to testify on Bill C-46, but you might be able to comment on how the interaction of Bill S-4 with Bill C-46 might operate. Bill C-46 is the technical assistance for law enforcement in the 21st century act, if you are familiar with that piece of legislation. How might that facilitate another tool?

C/Supt Stephen White: Unfortunately, I'm not familiar enough with it to present a position on how it interacts with Bill S-4 at this point.

● (1640)

Mr. Brent Rathgeber: Thank you.

There's a last question I have. I was quite interested when you talked in your presentation about the international identity fraud working group. I guess it goes without saying that this type of criminal activity knows no borders and that I am as likely to be ripped off by a white collar criminal in Europe or Venezuela as I am by one from across the street. Where are we with this whole international prosecution and reciprocal enforcement? If I'm the victim of an identity criminal from another jurisdiction, what recourse do I have or what recourse does Canadian law enforcement have?

C/Supt Stephen White: It's very similar to other types of criminal activity. In terms of working with the international community and facilitating criminal investigations, our most successful and used tool is the mutual legal assistance act. That's actually where we would request assistance from a foreign law enforcement agency.

You are right in that a lot of this activity is being perpetrated by individuals and organizations operating outside of Canada. We try to do our best to share information intelligence internationally between law enforcement agencies. As an example, for the next two days, Tuesday and Wednesday, we're meeting with our law enforcement counterparts in the United States and the United Kingdom to actually have this dialogue and to examine and explore further areas for cooperation on and facilitating international criminal investigations.

On a case-by-case basis, if there is a suspect in a foreign country and we need information or evidence from that country, we will proceed with a request under the mutual legal assistance act and treaty with that particular country.

Mr. Brent Rathgeber: Thank you. I hear the bell, so I assume my time is up.

The Chair: Yes.

Mr. Woodworth, for five minutes.

Mr. Stephen Woodworth (Kitchener Centre, CPC): Thank you very much, Mr. Chair.

This afternoon I heard the Privacy Commissioner reiterate something I found in a May 28, 2009, statement she made, to the effect that one in six Canadians have experienced some form of identity theft. That same report also indicated that over 90% of Canadians are concerned about identity theft.

I know this bill is substantially the same as Bill C-27 from the last session.

I've seen reports from PhoneBusters that in 2007 $6 million was lost to identity theft, and up until October 31, 2008, $8 million was lost. I've seen reports that Canadian banks and credit companies estimate that we lost $2 billion per annum. There are 1.7 million victims. So I was really pleased to hear comments from the Liberal member, Mr. LeBlanc, and also from the Bloc member, Monsieur Ménard, to the effect they think we need to pass this bill quickly.

I think Canadians can be glad that we have a government that has taken this problem seriously. It is a crime of the 21st century, it's been said, and I'm glad we have a justice minister who has taken it seriously.

[*Translation*]

Thank you to all of the witnesses.

[*English*]

I'm grateful for your attendance today. In particular, I admire Mr. MacRury as a good example of a prosecutor who knows that in law there is not a defence side or a prosecution side, but only justice, because some of the recommendations in the CBA report are what I would otherwise think of as defence recommendations.

I would like to focus in particular on the recommendation made on page 3 of the brief.

I will start with a question for Mr. MacRury about what is called *de minimus* behaviour in his brief, which is very close to the legal concept we have in our common law courts of *de minimis*. I am thinking that a lawyers' organization like the CBA would not likely toss out a term that is so similar, unless it might be intending to refer to the same thing; but I'm not sure, and I would like to know, to begin with, if in that recommendation you are talking about what a lawyer in the common law system would refer to as *de minimis* conduct in a criminal case.

Mr. Daniel MacRury: Yes, we are.

● (1645)

Mr. Stephen Woodworth: All right. That being the case, you are, of course, well aware that the courts in a common law jurisdiction at least already provide a *de minimis* defence against conviction if the facts warrant it. So I just want to know if your proposal would add anything to that.

Mr. Daniel MacRury: I'm very well aware of the common law. In fact, I'll give you a real-life example that happened 20 years ago. At that time, I actually was a legal aid lawyer. A person was charged with shoplifting a 2¢ screw from a store. The person was a 75-year old veteran who had never been involved in criminal law. This individual at that time had purchased something like $600 worth of goods, but he was charged because the institution had a pro-charge policy that any shoplifters had to be prosecuted, regardless of the amount.

That person was acquitted on that principle, but it should not have got to that point, quite frankly.

Mr. Stephen Woodworth: If I could stop you there, because our time is so limited, I just want to know if what you are proposing adds anything to the common law principle of *de minimis*.

Mr. Daniel MacRury: It builds it into the statute, which makes it clear to all the players in the system that this type of situation would not be caught.

I didn't mean to use up your time.

Mr. Stephen Woodworth: I have every confidence, Mr. MacRury, that if you or any experienced prosecutor were prosecuting, you would be very well aware of the *de minimis* principle in determining whether or not to proceed. So I am glad that you cleared up for me that this isn't intended to add anything to the common law *de minimis* defence, at least.

The second thing I'm curious about—

The Chair: Mr. Woodworth, you are out of time.

Mr. Stephen Woodworth: Oh, I'm sorry.

The Chair: You may get another chance, though, if we do have some time left.

Monsieur Petit, you have five minutes.

[*Translation*]

Mr. Daniel Petit (Charlesbourg—Haute-Saint-Charles, CPC): Thank you.

Good day, sirs. My question is directly mainly to the RCMP representatives. I may also have a question for Ms. Stoddart regarding a specific matter

Most likely you have read the bill now before the committee. I want to be certain that you understand me. Consider the following example. Some people have obtained and used a Quebec health insurance card, even though they do not live in this country. I'm sure you read about this in the newspapers. Thousands of people managed to obtain a health insurance card that entitled them to received free medical services paid by the residents of Quebec, even though they did not live in Quebec.

First of all, I would like to know if the bill will apply to fraud cases of this nature.

Secondly, we have another problem, one that is also occurring in Quebec. I'm not talking about Ontario, even though it has experienced the same thing. Foreigners managed to obtain social insurance cards that entitled them to receive a certain amount every month as well as free services. We are not dealing with identity theft in such cases. These individuals used the system fully to obtain benefits. You understand the difference.

Would the bill make it easier for the provinces or the federal government to take action against these individuals?

Ms. Jennifer Stoddart: I am not an expert in criminal law, but subsection 403(1) as amended by the bill notes the following:

> 403.(1) Everyone commits an offence who fraudulently personates another person, living or dead,

As I see it, the focus of this bill is NEXUS and identity theft.

I believe you are referring to instances of fraud and in my opinion, these are already dealt with in the Criminal Code.

Mr. Daniel Petit: My question was more specific than that, Ms. Stoddart. I am talking about people who come to Canada—either to Quebec or Ontario—under their real name. They obtain a health insurance or social insurance card and receive benefits in Quebec or in Canada, rather than in their own country. They are guilty of fraud.

In your opinion, will this bill make is easier to investigate such actions and will it perhaps provide for better sanctions against the people committing fraud? That is what I want to know.

● (1650)

Ms. Jennifer Stoddart: Sir, as I understand it, this bill deals specifically with identity theft. Therefore, if someone were to use a death certificate and pass themselves off as a Canadian who is deceased in order to obtain these benefits, then the provisions of this bill could apply.

However, I believe the Criminal Code contains other provisions that allow for the prosecution of individuals who have stolen someone's name or invented a fictitious person in order to obtain benefits. Perhaps the RCMP could enlighten us further.

[*English*]

C/Supt Stephen White: Yes, I do believe it would already be covered under the Criminal Code as uttering a forged document. So whether it be a health card or any other piece of identification or card that will get you an advantage, whether it be health care or some other advantage, it would be covered under uttering a forged document. I believe the revision of that in proposed subsection 368 (1) reads:

> Everyone commits an offence who, knowing or believing that a document is forged,
>
> (a) uses, deals with or acts on it as if it were genuine.

So it is covered under the current Criminal Code and would also be covered under the new revised provisions put forward here.

[*Translation*]

Mr. Daniel Petit: Thank you.

[*English*]

The Chair: Mr. Miller first, and then Mr. Comartin.

You have five minutes.

Mr. Larry Miller (Bruce—Grey—Owen Sound, CPC): Thank you very much, Mr. Chairman, and to all our witnesses.

Like Mr. Norlock, my question here is going to be on the theme of victims' rights or lack thereof. I've always felt that in a lot of our laws made by lawmakers like ourselves and enforced very questionably sometimes by our judges, the criminal's rights seem to be looked after more than the victim's rights.

This came about when I heard the comments on, I believe, section 25 and another section. I apologize if I don't have the right numbers. Mr. MacRury, you seem to have a problem with some of the aspects of that, which surprises me, because I strongly believe we should be giving the police all the tools they need.

I know in an example up in my own area of Owen Sound just a couple of years ago, police out doing regular patrols at 3 o'clock in the morning found a suspicious vehicle, which turned out to be loaded right to the roof with marijuana. That case got thrown out of court because of improper search and seizure. The public still shakes their head at that one. So I'm all in favour of anything we can do to give the police the tools they need.

We talk about the recouping of properties, or whatever, in order to reimburse the victims. If, under bankruptcy laws, a corporation or company can protect individuals from losing their personal property, does the same thing apply here under this law, when you can confiscate properties and what have you? I apologize if it sounds like a foolish question, but I'm not a lawyer, and I'd like to know if those same protections are there. I hope they're not, but I'd like to hear your comments on it.

Can a member of an organization be protected under the law if his organization, and he's a known member of it, commits a fraud?

C/Supt Stephen White: I guess in terms of the proceeds that would be generated from that fraud, there are provisions under proceeds of crime to attempt to seize and eventually forfeit those gains as proceeds of a criminal activity. They can be forfeited, obviously, to the crown. I'm not able to speak to what discretion a judge would have in terms of applying that in terms of restitution to victims.

Even if a fraud is committed by an individual in an organization, if those proceeds have been passed on to other individuals and through our investigation we can trace those proceeds, even if those proceeds have gone through two or three hands, which we call a laundering process, if we can still show the original source of those funds or proceeds from the criminal activity, we can attempt to have them forfeited as proceeds of crime, as proceeds of criminal activity.

● (1655)

Mr. Larry Miller: That's good. I'm glad to hear that.

Mr. MacRury, do you want to comment on my earlier point that you seem to have a concern about the police having too much...?

Mr. Daniel MacRury: Thank you.

The CBA position is very clear that one law should apply to everyone. We acknowledge that there are existing sections under section 25 of the Criminal Code, but those sections have procedural safeguards. Any time any individual breaks the law, there have to be safeguards. I would submit to you that the existing Criminal Code provisions have the proper procedural safeguards already in place. Any time you make exceptions to the rule of law, you have to be very prudent.

I would submit that the CBA position is very clear, and has been clear, that one law should apply to everyone and the procedural safeguards that exist in the existing Criminal Code are sufficient.

The Chair: We'll move on to Mr. Comartin, for five minutes.

Mr. Joe Comartin: I just can't let Mr. Woodworth's comments go by, praising the government and the current justice minister. The reality is that this bill would have been law by January of this year if we hadn't had an election and a prorogation of Parliament last year at this time.

Mr. MacRury, on the recklessness issue you raised, I had caught that as well, and I caught it last year before the election. You've used some terminology out of the Hamilton decision. Are you proposing that we use that type of wording? You weren't more specific other than that we need to look at it again.

Mr. Daniel MacRury: As I indicated earlier, there needs to be some clarity on this term. By fixing the clarity on that, you would strengthen the bill. The words in Hamilton are "substantial unjustified risk". If I were making a suggestion to the legislators, that would certainly be more explicit language that would be of assistance so there would be no doubt. If I put my other head on as a prosecutor, at the end of the day this bill has to actually work. We don't want to be spending our time in court basically fighting over the term "reckless". That's why clarity is important.

Mr. Joe Comartin: Are we at some risk that if we stick with "reckless" we will get a challenge that it's not specific enough and it will get struck down?

Mr. Daniel MacRury: In Hamilton it referred to another case at paragraph 33. The court went on to say that they were not going down that road of interpreting "reckless". The concern is that given it hasn't been interpreted by the courts; it's an open question. You have an opportunity as a legislature, if you so choose, to make more specific language so there's more clarity.

Mr. Joe Comartin: Maybe there are at two risks. They either strike it down because it's too vague, or the courts interpret it so rigidly that it doesn't accomplish what we're trying to accomplish in this section. Are those the two risks?

Mr. Daniel MacRury: Any time there is an interpretation, not certainty, there's that risk. Given that we're now at the legislation drafting stage, you have an opportunity to be more specific. That's what we're saying.

Mr. Joe Comartin: Thank you, Mr. Chair.

The Chair: Thank you.

We've basically gone through everybody at committee. Is there anyone who still has a question?

Mr. Woodworth, I cut you off earlier. Do you want to close with your second question?

● (1700)

Mr. Stephen Woodworth: Thank you very much.

On Mr. Comartin's comments, I recall that one of the reasons there was an election last year was that so much of the government's justice agenda got clogged up in the Senate and in the Commons. But I'm very happy that the NDP is working with the government to try to avoid an unnecessary election at this time.

I'll move on to the recommendation to expressly exclude the general provisions of attempt and counselling. I'm not really sure if the CBA is proposing that an attempt to steal identity information should not be a criminal offence. Is that what's intended by that?

Mr. Daniel MacRury: It's already there, and earlier testimony talked about a different overlap. The CBA's position is clear that where there is overlap there should be more clarification of "attempt" in the section. We are saying we should bring clarity to some of the overlap provisions of the code.

Mr. Stephen Woodworth: Do you see an existing provision that says an attempt to steal identity information is an offence? Maybe I've missed that, but without the general provision I'm not seeing it.

Mr. Daniel MacRury: To try to make some clarity, page 3 of our brief indicates that such preparatory acts may already be prosecuted using general attempt or counselling provisions of the code. Given this overlap in the relationship between the proposed new provisions and the existing provisions, it should be clarified to avoid unintentional broadening or breach of the law. So we're saying there is a potential overlap.

Mr. Stephen Woodworth: Maybe I'm just being dense. I have to tell you that at the moment there is no offence of stealing information—an intangible. There is no attempt for that offence either. Once this bill is passed, it will be an offence to steal identification information, but I can't see any reason why the general provision regarding attempts or counselling should not apply. If you have any further comments that are not available today to help me with that, I would appreciate it.

Thank you.

The Chair: Thank you.

I think we've heard most of the questions. I'll just close with one of my own.

Most of you probably know that our committee has been undertaking a comprehensive review of organized crime. We're hoping to issue a report either later on this fall or perhaps early in the spring. My question to anyone who can answer is, what proportion of ID theft is actually committed by organized crime or those serving organized crime? Do we have those statistics? Do our RCMP witnesses know?

Insp Kerry Petryshyn: I don't have any specific statistics to break it down simply because of the fact that we have such limited data with regard to how many offences are really taking place out there.

As was mentioned earlier on in the meeting, the number from the Canadian Anti-Fraud Call Centre is only a small sliver of what's really taking place out there. But what I can say is that what I'm seeing nationally from our analytical unit, who piece together what might be hundreds of seemingly unconnected complaints into a common group, is that anywhere between 70% and 80% of the complaints we see are connected to some sort of organized crime group.

The Chair: That's very significant. That's greater than I thought it would be.

I have a follow-up, and I'm surprised Mr. Comartin didn't ask this question. Mr. Comartin does want to bring a witness to the table dealing with the whole issue of title fraud. Is that something you're encountering more? I know the various provinces have different land title schemes. I know my own province of British Columbia has imposed upon us as lawyers a much greater onus to confirm the identity of our clients. But that's only part of the solution.

I'm wondering, will the legislation that you have before you today assist you in tackling title fraud?

● (1705)

C/Supt Stephen White: It will assist us in that we will have a tool if we do identify someone using another person's identification to attempt to advance a title fraud. There will be a provision in here, “possession of that identification”, that we can use at the outset, hopefully before the actual title fraud has been carried out.

As I said earlier, for us the great tool of this piece of legislation moving forward is that it gives us a very precise and tangible tool that law enforcement can use at the front end of a wide spectrum of identity fraud activities.

The Chair: Does anybody else have any questions? If not, I want to thank our witnesses. Your testimony has been very helpful, and we'll certainly take it under advisement and move forward with this legislation.

Mr. Joe Comartin: Just before you adjourn, I'm concerned that the title insurance people weren't here today. I understood from the work my office had been doing with them that they did want to appear. There had been contact with the clerk of this committee. I saw the list this morning and they weren't on, and I don't know what has happened. It may be that they could not make this meeting. I still believe we should give them the opportunity to appear.

So in our scheduling over the next week or two, I would like to see that they come back and that Bill S-4 is on, even if it is for a short period of time, at another meeting.

The Chair: Mr. Comartin, I believe you were going to connect with our regular clerk. We will do everything we can to accommodate the witness if that witness wants to appear. I think we can do that.

This meeting stands adjourned to the call of the chair.

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

SPEAKER'S PERMISSION

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

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

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

PERMISSION DU PRÉSIDENT

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

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