HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 018 • 2nd SESSION • 41st PARLIAMENT

EVIDENCE

Tuesday, April 8, 2014

Chair

Mr. Pat Martin

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, April 8, 2014

● (1100)

[*English*]

The Chair (Mr. Pat Martin (Winnipeg Centre, NDP)): Good morning, ladies and gentlemen. We'll convene our meeting.

Welcome to the 18th meeting of the Standing Committee on Access to Information, Privacy and Ethics.

Today we continue our study on the growing problem of identity theft and its economic impact.

We're pleased to welcome, as witnesses and presenters today, representatives from the Canadian Human Rights Commission, Mr. Philippe Dufresne, director general and senior general counsel; and from the Canada Revenue Agency, Ms. Susan Gardner-Barclay, the assistant commissioner and chief privacy officer, who is accompanied by Helen Brown, director general for security and internal affairs directorate.

We will begin with opening remarks from both of the parties. We'll begin with Mr. Dufresne, from the Canadian Human Rights Commission.

Usually, we invite you to make a presentation of approximately 10 minutes and then we open it to questioning from the floor.

Welcome, Mr. Dufresne. You have the floor.

Mr. Philippe Dufresne (Director General and Senior General Counsel, Human Rights Protection Branch, Canadian Human Rights Commission): Mr. Chair, thank you to the committee for inviting the Canadian Human Rights Commission to contribute to your study on the growing problem of identity theft and its economic impact.

I would like to introduce my colleague, Maciej Karpinski, senior research analyst with the commission's protection branch.

Today, I would like to touch upon three main points. First, I will briefly talk about the Canadian Human Rights Commission and how we promote and protect human rights, and ensure equal opportunity for Canadians. Second, I will discuss the commission's 2010 report on identity certification and the importance of ensuring that measures used to certify a person's identity comply with human rights principles. Finally, I will share with you our recommendations on how to avoid being discriminatory in this area.

[*Translation*]

I will begin with a short description of the commission and its mandate.

We are mandated by Parliament to administer the Canadian Human Rights Act and monitor compliance of federal organizations with the Employment Equity Act.

We receive discrimination complaints regarding employment and services provided by organizations under federal jurisdiction. This includes the federal public sector, as well as private sector companies involved in industries such as transportation, telecommunications and banking.

We also participate in major human rights cases before tribunals and courts, including the Supreme Court of Canada.

The commission works to prevent discrimination and promote the development of sustainable human rights cultures. We do this by providing organizations with research, policies and tools to promote understanding of and compliance with the Canadian Human Rights Act.

One of these tools is the Human Rights Impact Assessment for Security Measures, which I will touch upon later in my remarks.

[*English*]

The report you have asked us to speak about today was published in 2010. It was part of a research initiative related to national security and human rights. Our objective then was to help national security organizations strengthen their identity certification practices in a way that respects human rights principles.

While our report focused on national security organizations, its conclusions, we believe, are relevant for any public or private organization that offers services for which identity information is required. We therefore hope that the information contained in this report will be of assistance to the work of this committee.

[*Translation*]

Our report demonstrates that the most common forms of identity certification tools used are at risk of being discriminatory based on the prohibited grounds of discrimination set out in the Canadian Human Rights Act. And that is for two reasons.

First, the method may be inaccessible to an individual or a group of individuals. Second, discretionary decisions rendered by officers in validating identities may lead to discrimination.

[*English*]

Our report has shown that there are two main types of metric systems used for identity purposes. The first is uni-modal, which is using just one metric of identity information, and the second is multi-modal, which is using a combination of two or more metrics.

For example, a uni-modal system might rely exclusively on fingerprints. This may be inaccessible to people who do not have fingers or whose fingerprints have been affected by their working conditions and/or their age. By contrast our study found that multi-modal biometric systems offer a degree of inclusiveness that can often address the limitations of uni-modal systems. Multi-modal systems not only have the capacity to help protect human rights, but also have the ability to build a stronger and more trustworthy security system.

At the time of the review, the personal identity certifier card in the United States was identified as an effective multi-modal system. This card stores both fingerprints and facial-scanned biometrics for each enrolled federal employee or contractor. Though it primarily uses fingerprint biometrics, digital facial imaging is used when it is not possible for a federal employee or contractor to provide fingerprints, or if there is an anomaly.

In dealing with these important issues, human rights law provides guidance for determining whether an otherwise discriminatory measure can be justified. This includes looking at: first, the extent to which the measure is necessary; second, whether there are less discriminatory ways of achieving the same objective; and third, the extent to which the infringement on human rights outweighs the benefits gained by the measure.

Situations may also arise where users may require an exemption. Policies and practices to reasonably accommodate these individuals should therefore be included as part of the development of any measure. Should there be no reasonable alternative for a given biometric, it is up to the organization employing the biometric to demonstrate that sufficient measures have been taken to explore other less discriminatory ways of achieving similar results.

Based on these principles, we developed the human rights impact assessment for security measures. This tool outlines the steps to take during a security measure's life cycle to ensure that security standards, policies, and practices are both effective and respectful of human rights.

● (1105)

[*Translation*]

We believe that by applying a human rights impact assessment before a security measure is finalized, we can not only improve a security measure's effectiveness and efficiency, but also save time and money while bolstering public support for new and existing security initiatives.

That is what we mean when we call on organizations to apply a human rights lens to a proposed policy or procedure.

[*English*]

Thank you for your attention. We'd be happy to take your questions.

The Chair: Thank you, Mr. Dufresne.

We'll go now to Susan Gardner-Barclay, from the Canada Revenue Agency.

You have approximately 10 minutes, please, Ms. Gardner-Barclay.

Ms. Susan Gardner-Barclay (Assistant Commissioner and Chief Privacy Officer, Public Affairs Branch, Canada Revenue Agency): Good morning, Mr. Chair, and thank you very much.

Good morning to members of the committee.

My name is Susan Gardner-Barclay, and I am assistant commissioner of the public affairs branch and chief privacy officer of the Canada Revenue Agency, or CRA.

I am joined this morning by Helen Brown, our director general of the security and internal affairs directorate at the CRA's finance and administration branch.

[*Translation*]

We are very pleased to appear before you today to support you in your study on the growing problem of identity theft, by speaking about the measures the CRA has in place to protect taxpayer information.

[*English*]

As one of the Government of Canada's largest institutions, the CRA has more interactions with Canadians than any other department. In 2012-13 alone, over 27 million Canadians and businesses filed tax or benefit returns. The CRA collects approximately $400 billion annually in taxes and duties, and distributes $22 billion in credits and benefits to Canadians. Our call centres receive 20 million calls a year, and we process over 150 million pieces of mail. As a result, we have one of the largest personal information data holdings in the Government of Canada.

The trust that Canadians place in the CRA to protect their information is the cornerstone of Canada's system of voluntary self-assessment. Further, section 241 of the Income Tax Act and section 295 of the Excise Tax Act prohibit the disclosure of taxpayer information by any employee of the CRA unless specifically authorized under these acts. Breach of these provisions is a criminal offence subject to strong penalties up to and including imprisonment.

[*Translation*]

That's why the CRA has an extensive number of safeguards in place to protect Canadians' personal information and, in turn, reduce the risk of identity theft.

First and foremost, the agency has worked diligently to promote a strong culture of integrity among its employees.

● (1110)

[*English*]

Our code of ethics ensures that staff are aware that the protection of the privacy rights of taxpayers is central to their responsibilities and that this responsibility continues even after they leave the CRA.

In 2012, the CRA launched its integrity framework, all of its policies, programs and systems that work together to protect the integrity of the agency. The framework ensures that the high standards established to protect taxpayer privacy are communicated to all employees and managers, and that the CRA's performance against those standards is carefully monitored and reported.

The CRA also works closely with the Privacy Commissioner of Canada to ensure that protections are strong and any areas of improvement are addressed.

In 2009 and 2013, the Privacy Commissioner conducted audits of the CRA's privacy management regime. In these audits, the commissioner recognized the immense scope and complexity of the CRA's operating environment, as well as the agency's established culture of security and confidentiality. Of course, she also noted areas for improvement that focused on the consistent and timely completion of privacy impact assessments; the completion of risk assessments for all IT systems that process taxpayer information; strengthened monitoring of employee access to CRA computer systems; and improved processes for sharing information internally about privacy breaches. The CRA agreed with all recommendations, and significant progress has been made in responding to them, with many activities already completed.

[*Translation*]

This includes the creation of the role of chief privacy officer in April 2013. I assumed that role when I was appointed as Assistant Deputy Commissioner of the Public Affairs Branch and Chief Privacy Officer in October of last year.

[*English*]

As chief privacy officer, I am responsible for overseeing all decisions related to privacy at the CRA and to champion and report on personal privacy rights within our organization.

The CRA is also actively pursuing many other program, policy, and technology changes to strengthen our privacy management. These include building on our front-end controls that ensure employees have only the access to CRA computer systems that they require in order to perform their duties, and strengthening our back-end controls to build on our automated systems so that the CRA can better monitor and analyze the full range of actions performed by employees on their computers.

New information-sharing protocols have also been established within the agency to ensure accurate reporting and monitoring of privacy issues, and we have put in place an integrity advisory committee, chaired by the commissioner of the CRA, with an external integrity adviser as part of its membership. We are also conducting an organization-wide exercise to verify that privacy impact assessments are up to date for all agency programs or initiatives requiring one.

The CRA is keenly aware that, due to the nature of the information holdings we have, a breach of personal information may hold the potential for that information to be used in identity theft or other criminal activities.

The nature of information breaches that occur at the CRA is extremely varied, and can range from an employee mistakenly accessing the wrong taxpayer file in the course of his or her work, to misdirected mail, which in fact, constitutes 95% of the CRA's information, data and privacy breaches, and to rare instances where the personal information accessed could potentially be used for fraud or financial gain.

It's important to note that many of the breaches identified by the CRA do not constitute privacy breaches, as no personal information was disclosed. However, when the CRA discovers a privacy breach has occurred, the breach is assessed in accordance with Treasury Board policies and procedures to document and evaluate all potential risks to the affected individual.

In instances where there is reasonable potential that an individual may have been harmed by the privacy breach, that individual is informed. The Privacy Commissioner is also informed according to Treasury Board guidelines.

Before I conclude, I'd like to take a few moments to address what the CRA does to warn Canadians about third party phishing schemes that attempt to masquerade as the CRA in order to gain sensitive personal information from the victim. This year's tax season has seen a significant growth in these types of schemes and the CRA continues to take a variety of measures to warn Canadians about them. Our website provides easy to find information on what these scams look like and what to do to reduce the risks of identity theft. We also use tax alerts and news releases to the media, and frequently highlight this information to Canadians through our corporate Twitter account.

To reach communities such as seniors or other vulnerable groups who may not have access to the Internet, we have a proactive media strategy that offers interviews to specialized media, and in a variety of languages depending on the region, including Punjabi, Hindi, Cantonese, Greek, and Italian. We also have a strong network of intermediaries, seniors and youth organizations, multicultural groups, police associations, tax preparers, among many, who distribute our information to their clients and communities. We partner with other government organizations to spread the word through such events as fraud prevention month. When identity theft does happen, the CRA can and will flag taxpayer files to guard against suspicious activity.

In short, Mr. Chair, the CRA is working to ensure controls are in place, and that we continue to assess and improve those controls.

● (1115)

[*Translation*]

Our responsibility to protect Canadians' information is fundamental to who we are and what we do, and we continue to dedicate significant effort to meeting the expectations of Canadians in this regard.

[*English*]

We'd be very happy to take your questions.

The Chair: Thank you, Ms. Gardner-Barclay.

We'll go to rounds of questions.

For the official opposition and the first seven-minute round, Charmaine Borg.

[*Translation*]

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

First, I'd like to thank our witnesses for joining us today. Even though you are all undoubtedly very busy, you took the time to come and speak to us about a very important issue. We really appreciate it.

Now, I'd like to ask the Canada Revenue Agency officials a question.

In your presentation, you indicated that a number of data breaches had occurred. In response to a written question from a colleague of mine, within your department, you identified 2,983 occurrences of data breach or loss affecting 2,249 individuals. That represents more than half of data breaches or losses if you consider all federal agencies in question. That's extremely high for a single year.

With so many data breaches or losses, how do you intend to do a better job of managing Canadians' personal information and reduce the risk of identity theft that data breaches can lead to?

[*English*]

Ms. Susan Gardner-Barclay: Let me begin by giving you a bit of context around the numbers that appeared in written question 255, which I think is the question you're referring to.

That response indicated that the CRA had experienced around 2,900 information, privacy, and data breaches in the time period requested. Some 2,800 of those were actually misdirected mail. That constitutes about 0.001% of the 150 million pieces of mail that the CRA handles in any given year.

Having said that, we certainly understand that we need to take strong measures in any instance where a taxpayer's information ends up where it shouldn't be. We do have measures that are aimed at addressing misdirected mail specifically, and my colleague Helen Brown can speak to that.

I'll also mention the number of initiatives that we have put in place as a result of the two Office of the Privacy Commissioner audits we had in 2009 and 2013, which I referred to in my opening remarks.

We essentially now have a tiered response to managing information security and privacy breaches.

Our first line of defence, of course, is our employees. We have a very strong code of conduct that makes it absolutely clear to our employees what their responsibilities are with regard to security management.

We have ongoing staff training and awareness. We have a mandatory course for security for all of our employees at the CRA. We now have extensive information-sharing protocols within the CRA that help us to identify and address breaches when they do occur, particularly between our security and advisory directorate and our ATIP directorate, which has responsibility for monitoring these things.

We now have active controls at the front end of our technological systems which ensure that only the computer systems that employees need to access to do their jobs are those that they can access. We now have very strong back-end controls and are working to actually strengthen those through some technological changes that we'll have in place over the next two years We will put in place systems that will allow us to very carefully monitor employee activity on all of our computer systems, right down to what files they're accessing, how they're accessing them, and what information they're looking at on those files.

We have a very strong regime of policies and practices that go along with that, including a very strong discipline policy that situates unauthorized access as a significantly serious offence within the disciplinary regime. We have a very strong oversight process, which includes my office. It includes the integrity advisory committee that I referred to, and of course, the OPC, which takes great interest in our privacy regime.

[*Translation*]

Ms. Charmaine Borg: Thank you kindly.

Ms. Brown, you may have a chance to answer my next question.

Ms. Gardner-Barclay said that 2,800 pieces of mail were sent to the wrong person. A constituent of mine came to see me with a letter telling him he was now eligible for old age security. With his letter was another one addressed to someone else. Clearly, both letters contained very confidential information. And I, myself, alerted the CRA about the situation.

If it happened in my riding, I assume it has happened to many people. You said 2,800 were affected. What do you do when that happens? Why were 2,800 pieces of mail sent to the wrong person?

You said it represented a low percentage of all CRA mail, but it still seems like a lot of people to me. We are talking about 2,800 people whose identities could potentially be stolen as a result. And to me, that's very serious.

● (1120)

[*English*]

Ms. Helen Brown (Director General, Security and Internal Affairs Directorate, Finance and Administration Branch, Canada Revenue Agency): Thank you for your question.

It's a very important issue. Our goal would be to have no misdirected mail, if that were possible, and we've put many steps in place.... I don't know when your situation occurred personally, but what we've put in place in the last year is a protocol whereby as soon someone advises us that there has been misdirected mail, our security people get back to them within a day and we find a way to retrieve the misdirected mail.

Our norm is that we're getting it back within four days. Of the mail that's misdirected, we manage to retrieve 95%. We look to see what the cause of the problem was so that we can try to reduce the risk of its happening again, and we advise the taxpayer, if we feel that there's been the potential for harm.

[*Translation*]

Ms. Charmaine Borg: How do you keep it from happening?

Let's say I receive a letter from the old age security people as well as someone else's letter. If I were a person who was up to no good, I could use the confidential information in the letter to steal the person's identity.

How can you assure the beneficiary that the person who received their letter erroneously isn't going to use the information in the letter for criminal purposes?

[*English*]

Ms. Helen Brown: My first response to that question is that as our first line we would try to retrieve it as quickly as possible. The second thing, if we find out about the misdirected mail, is that we advise the taxpayer, if we think there's a risk of harm, and encourage them to contact the CRA. We can either provide them with some support with Equifax, the credit services, and/or we can put a flag on their file so that we are aware that there's a concern there might be identity theft.

The Chair: Thank you, Ms. Brown.

I'm sorry, Ms. Borg, that concludes your time.

Next, for the Conservatives, is Mr. Laurie Hawn.

Hon. Laurie Hawn (Edmonton Centre, CPC): Thank you to all the witnesses for being here.

I'd like to talk a little bit more about the impact of these things, rare as they are—and that's a good thing. Just to refresh the numbers—this is for CRA—did you say that 150 million pieces of mail go out?

Ms. Susan Gardner-Barclay: There are 150 million pieces of mail that we manage; around 120 million of that correspondence is correspondence coming from the CRA, and the remainder is correspondence coming back in to the CRA. It is 150 million in total.

Hon. Laurie Hawn: I think you said that 0.001% of the things that you send out wind up being misdirected.

Ms. Susan Gardner-Barclay: That's correct.

Hon. Laurie Hawn: What's the raw number? Was that the 5% of the 2,800?

Ms. Helen Brown: That's a good question.

Ms. Susan Gardner-Barclay: It's about 1,600.

Hon. Laurie Hawn: Okay.

Are there any cases of any of those misdirected pieces of mail falling into the wrong hands? The number of bad people out there who would take advantage of this is pretty small, and the chances of that piece of mail going to one of those people is really very small. Has there ever been a case of misdirected mail having an actual negative impact on a taxpayer?

Ms. Susan Gardner-Barclay: We have no evidence that that this has ever occurred. A significant majority of the misdirected mail that is sent out doesn't actually contain any personal information, as well.

Hon. Laurie Hawn: To Ms. Borg's question, which is a legitimate hypothetical question, the odds of that happening are pretty tiny, I would suggest.

With respect to the kind of experience you had with human rights, I'm not sure how you would characterize the impact. I see three things: somebody might use information for extortion purposes of some kind, or simply for identification theft, or for fraud against a vulnerable senior or something like that.

Do you have any data on the frequency of any of those kinds of things?

Mr. Philippe Dufresne: We have not looked into the frequency of theft or the frequency of use of information that might have been stolen. What our report focused on was what types of information we're using and what types of metrics we're using to certify the identity of Canadians, whether to gain access to services or access to Canada, etc., and whether those measures are having a negative human rights impact, and what we can do to prevent negative human rights impacts.

We found that ensuring that measures are consistent with human rights principles is not done at the expense of security; it strengthens security. They work together.

● (1125)

Hon. Laurie Hawn: Okay.

I have a question for both agencies. A lot of work, obviously, has gone into keeping information secure, and every agency does its own thing. How much information sharing on best practices goes on between agencies such as the Human Rights Commission, Public Safety, CRA, and so on?

Either of you may respond.

Ms. Susan Gardner-Barclay: We participate quite actively on two levels. The first is around the access to information community. We participate in interdepartmental standing meetings of ATIP personnel. Information is exchanged on best practices. As a matter of fact, we recently gave a presentation to other departments on the creation of the chief privacy officer and its mandate in other departments. Also, Ms. Brown participates in a similar community of departments that look at departmental security measures.

Ms. Helen Brown: To elaborate on what my colleague just said, there's a strong group of departmental security officers around town who have frequent meetings to share best practices, Actually, the CRA is one of the groups that shares our best practices with others, because we're seen as a leader.

Hon. Laurie Hawn: Yes, you would be one of the biggest.

What is the situation for the Human Rights Commission?

Mr. Philippe Dufresne: We have a twin mandate at the commission of protecting human rights and promoting them. While we are a regulator and receive complaints and participate in cases, we also have a very strong mandate to work with stakeholders to promote, to research, and to share information. In so doing, we share information with departments such as the Department of Justice and with agencies.

In the context of this research, we consulted a number of national security agencies, including Foreign Affairs, Passport Canada, CIC, and we have shared our best practices with them.

In this case it was a question of trying to have options among methods for identifying Canadians and trying to gather information to see and ensure that discretionary decisions are not taken in a way that adversely impacts upon a given group.

Hon. Laurie Hawn: Okay.

In terms of staff discipline—just to put some meat on the bone, I guess—at CRA you have a very strict regime of oversight and screening, presumably, for anybody who comes into CRA.

CRA is one of those organizations that many people love to hate because you take their money. I get that. But you're doing a tough job and doing it well.

With all that oversight and all the measures you talked about, how often do you have a case in which somebody has to be disciplined, and what kind of discipline would be meted out?

Ms. Helen Brown: We have a discipline grid at CRA that tries to ensure that there is consistency in application, because we're such a large organization with approximately 40,000 employees. The grid will say what kind of misconduct has occurred and then what kind of discipline should be given.

For unauthorized access, it ranges from suspension up to dismissal. I can say that in the past year, there have been 14 employees dismissed and 18 suspended for that reason.

Hon. Laurie Hawn: Out of 40,000, that's a low percentage. Do you have any comparators for measuring against other large government organizations?

Ms. Helen Brown: No.

Hon. Laurie Hawn: Your job is rather unique.

Ms. Susan Gardner-Barclay: I think the numbers reflect that we take the problem quite seriously and follow through when incidents occur and that there is some consistency across all of our branches in ensuring that the issue is recognized and treated in a consistent fashion.

Hon. Laurie Hawn: I know you have to abide by all normal labour codes and so on, but how difficult is it—this is a subjective question looking for a subjective answer, I guess—to fire a PSAC employee?

Ms. Susan Gardner-Barclay: I'm not in a position to comment on that. I think the evidence speaks for itself, in that it shows that it has happened.

An hon. member: I have a point of order.

The Chair: Excuse me, but we have two issues. First of all, you're out of time, Mr. Hawn, but second, there's a point of order from Madame Borg.

[*Translation*]

Ms. Charmaine Borg: Mr. Chair, I don't think the question is relevant to our study. Knowing how difficult it is to fire an employee has no bearing on identity theft.

● (1130)

[*English*]

The Chair: Your point of order is one of relevance, but the problem has solved itself because Mr. Hawn has to stop that line of questioning right now.

I think you do have a legitimate point of order, by the way.

Next, we have Mr. Regan for the Liberal Party.

Welcome, Mr. Regan. You have seven minutes.

Hon. Geoff Regan (Halifax West, Lib.): Thank you very much.

[*Translation*]

I'd like to begin with a question for Mr. Dufresne.

You mentioned that the United States has personal identity certifier cards that use biometrics. I've heard about devices that can erase the information on the card when you walk in front of them. What is the best way to prevent that, in your view? How much attention do you pay to the matter?

Mr. Philippe Dufresne: We've shared a tool with a number of the organizations we work with. It's a guide on the impact of security measures on human rights and is intended to address issues just like that. It examines whether persons with disabilities and members of other groups protected under the act have access to the measure in place. That analysis has to happen at the very beginning when the measure is first implemented. Then, the measure has to be tested to determine whether it is effective security-wise and whether it has a negative impact.

The situation you described would involve an impact. The test could reveal that the measure seemed like a good idea initially but had a negative impact on either safety, health or individuals.

And the assessment process should continue even after the measure is implemented. Assessment and improvement have to be ongoing.

[*English*]

Hon. Geoff Regan: So it wouldn't make a distinction in the sense, I suppose, there's not.... You don't think of a way offhand that this kind of activity, trying to steal someone's information with that kind of a scanner, would discriminate against the people that you have to be concerned about.

Mr. Philippe Dufresne: Every situation, we say, ought to be looked at for its human rights impact.

If you have a situation where you find that a certain protected group, say, persons with disabilities, is more likely to have their identity stolen with a given measure, then that impact ought to be identified. It then raises the question, how can we minimize and at best eliminate that negative impact? That's what the human rights impact assessment is. We look at groups. We're not only looking at a direct impact on the group but indirect as well. Let's make sure, and again, this shouldn't impact security, as security is fundamental, but let's make sure that the human rights lens is there from the very design of the measure throughout its implementation and beyond.

Hon. Geoff Regan: My understanding is that you can put your credit card or other kinds of cards and that kind of information in a secure folder. There are some wallets that will protect you from that and others will not. A lot of people would know that but lots wouldn't, so getting that information out would be important.

You suggested that multi-modal methods of confirming identification are better. Can you give some examples of those methods and of some institutions or companies that use them?

Mr. Philippe Dufresne: The one that I gave was the personal identity card in the United States. This was one where you're using fingerprints. If that doesn't work, you're going to use facial recognition.

Hon. Geoff Regan: Are there any in Canada that you could think of?

Mr. Philippe Dufresne: I'll ask my colleague, Mr. Karpinski, if this came out in the research.

Mr. Maciej Karpinski (Senior Research Analyst, Human Rights Protection Branch, Canadian Human Rights Commission): There are a few examples in Canada.

If you look at the report, we surveyed a bunch of secondary identity documents produced by the Government of Canada. Among them is the NEXUS card which uses two particular biometrics, that being fingerprinting and iris scans. There's an example that, should the fingerprint not be readable or the person not have the appropriate fingers in order for the machine to scan, they could potentially rely on an iris scan. That in itself might not necessarily be as inclusive because not everybody might have scannable fingers and scannable irises. It's to ensure....

What the report demonstrates is that when you develop those kinds of systems, you always have some kind of additional thinking behind it to say that if this is what is required, what other measures can you put in place that might compensate for those exceptions where needed?

There are other simpler examples. If you go to a grocery store, for example, you might find hand scanners that allow you to clock in an employee. There again you might want to find out if the hand scanner can scan one hand or both hands. You want a system that can scan presumably both because there have been demonstrated examples of people objecting to having one particular hand scanned over another. When you have systems like that, our argument is to not rely exclusively on that one system, but have others there to complement it.

● (1135)

Hon. Geoff Regan: I'm trying to think of how I can speak as a left-hander and object to something or other but I can't offhand think of any particular example.

Mr. Maciej Karpinski: The example is in the report. There's a case that is referred to. There are certain religious practices that lend themselves more toward scanning with one hand and not both hands, or with the other hand.

Hon. Geoff Regan: Thank you very much.

Ms. Gardner-Barclay, I think you probably told us this already, but when you referred to the 2,900 breaches, what period were you talking about?

Ms. Susan Gardner-Barclay: It was for the year 2013.

Hon. Geoff Regan: So that was for one year.

Ms. Susan Gardner-Barclay: Yes.

Hon. Geoff Regan: What process was in place before that to prevent this from happening?

Ms. Susan Gardner-Barclay: We actually had many processes in place to prevent it from happening. As a result of this, and particularly around the OPC's report from 2013, we strengthened those processes. But we did have front-end controls that looked at managing carefully employee access to CRA systems.

We do have back-end controls. We are putting a system in place over the next two years that will strengthen that. We do have the ability to monitor employee access to our systems and what information they're looking at.

All through 2010 to 2013, we revised our privacy policies and procedures. We implemented a new discipline policy. We strengthened our training and awareness programs for employees. That began in 2010 and continues, but the bulk of that work was done over the last three years.

Hon. Geoff Regan: The vast majority of these were, as you say, misdirected mail.

Ms. Susan Gardner-Barclay: Correct.

The Chair: Geoff, you're out of time.

Hon. Geoff Regan: Already?

The Chair: You're well over time, actually. I cut you a lot of slack because you're new. You'll have to continue that in the next round.

The last questioner for the seven-minute round is Pat Davidson.

Mrs. Patricia Davidson (Sarnia—Lambton, CPC): Thanks to our witnesses this morning. These certainly are interesting things you are filling us in on.

I want to start with a quick question for the CRA, please. You stated in your opening comments, “It's important to note that many of the breaches identified by the CRA do not constitute privacy breaches, as no personal information was disclosed.”

How do you define “personal information”?

Ms. Helen Brown: Perhaps I can answer that.

Private information is about an individual. We were distinguishing between that and breaches that could be information about a business, for example, a piece of mail with the business name and address, which is public information. We would have considered that a breach of information but not necessarily a breach of privacy.

I don't know if that explains it.

Ms. Susan Gardner-Barclay: Perhaps I can add to that.

In order to define privacy breaches, we rely on the Treasury Board guidelines. The Treasury Board guidelines define a privacy breach as an improper or unauthorized collection, use, disclosure, retention, or disposal of personal information. Anything that is outside of that category we would define as an information and data breach, but not a privacy breach.

Mrs. Patricia Davidson: Would you classify personal information then as an individual's name, address, birthdate, SIN?

Ms. Susan Gardner-Barclay: Yes.

Mrs. Patricia Davidson: Okay. But if it's a company's name and address that is publicly available, that's a different situation.

Ms. Susan Gardner-Barclay: Yes. It's when the name and address are publicly available on public databases. Exactly.

Mrs. Patricia Davidson: Okay.

In your opening remarks, you also referred to section 241 of the Income Tax Act and section 295 of the Excise Tax Act prohibiting disclosure of taxpayer information by any employee unless specifically authorized under these acts.

What does that mean? What would be specifically authorized?

● (1140)

Ms. Susan Gardner-Barclay: The act does permit some disclosure, if authorized. The most clear example would be if you have the consent of the taxpayer. There are some instances where the taxpayer is providing consent for their information to be disclosed to another party.

A good example of that would be that authorized representatives, income tax companies which prepare returns, need to have the taxpayer's consent to share that information with them. That's the most obvious example.

Mrs. Patricia Davidson: In an MP's office, working for a constituent, we need to have a consent form signed.

Ms. Susan Gardner-Barclay: That's correct. That would be another instance. We have a consent form. Taxpayers will complete that form, and their MPs will complete that form, and send it to us. That's the mechanism by which we are then permitted to share confidential taxpayer information with an MP who's representing a taxpayer.

Mrs. Patricia Davidson: Okay.

I had a constituent express some concerns to me last weekend. Of course we all know it's income tax time, and we're all hustling to get our returns prepared. This individual had used a particular preparer for several years, had some issues, and decided to go to a different preparer this year.

They went to the second preparer, and they took along their previous information so that they could share their past returns with the new group. They were told they didn't need to worry about that, because all the new preparer had to do was go online and they could access all of the past returns.

Is that correct?

Ms. Susan Gardner-Barclay: This is a little outside our area of expertise, but the second tax preparer would have to have obtained authorization from the taxpayer to be able to access any of the information that is available online. I am aware of no scenario where a tax preparer could simply find that information without obtaining the appropriate authorization. Our controls on this are very strict. We use the same technological controls that major Canadian financial institutions use to be able to manage access to that sort of information that may be available online.

Mrs. Patricia Davidson: When those files are sent in, are they kept at CRA, or are they kept at the tax preparers, or are they kept at both?

Ms. Helen Brown: Again, it's a little bit outside of our area of expertise, but CRA obviously needs to hold the information if it's to do with the CRA and to do with our taxes. I imagine the preparer would also need to have some record.

I'm not sure if that answers your question.

Mrs. Patricia Davidson: Yes, it does. I'm just a little bit concerned about how the taxpayer then...maybe there's something on the original tax preparer's form where they've given consent to share that information. I don't know, but maybe that's what the individual needs to be concerned about.

Ms. Susan Gardner-Barclay: We'd be happy to provide you with further information on that so that you have a good sense of what the framework is around how that would be managed.

Mrs. Patricia Davidson: I'd be interested in that. If you could send it to the clerk, that would be good. Thank you very much.

You talk about getting information out, reaching communities and vulnerable groups, and so on, and you talk about some of the different organizations that you partner with. I just have a suggestion, and maybe you already do it on a lot of things, but maybe it's not happening with some things. MPs are excellent people to partner with. We all have websites, and most of us are on social media of some kind with Facebook or Twitter, and most of us have lots of people following what we're doing. It's a good way to get things out. I know we received information on the phishing scams that were going on and that was something that put out, and it was very well received in the community. People want to know these things. So we're a good avenue to help you.

Ms. Susan Gardner-Barclay: I'll just add to that. We've always known it, but we took action on it last year for tax filing season when we in fact provided a member of Parliament kit on everything that your constituents need to know about the tax filing season. We did that last year, and we got an excellent response. There were literally thousands and thousands of access to those pages. We replicated it this year and it's having an even better response. This was sent out to the offices of all members of Parliament so that you would have it.

We gladly welcome any suggestions for improvement. We'll make sure that the information about phishing scams is included if it wasn't this year. I'm looking through the table of contents in my head, and I'm not sure it was there. I know it went separately, but we'll make sure it's part of that package next year.

● (1145)

The Chair: Thank you, Ms. Davidson. Your time was concluded.

Next we'll go to five-minute rounds, beginning with Mathieu Ravignat.

Mr. Mathieu Ravignat (Pontiac, NDP): This question is directed to the Canada Revenue Agency. Thank you for being here, Mesdames.

Maybe you can correct me if I'm wrong, but my understanding is that of the 2,983 incidents, only 1% of them were actually reported to the Privacy Commissioner. That represents about 1,700 Canadians, I think. Does this mean that those individuals have no idea what happened with regard to their data and whether or not this data can be stolen for purposes of identity theft?

Ms. Helen Brown: If I may start, I'm sure that my colleague will continue with the answer, but I just want to make one point of clarification. Of the 2,983 breaches that we reported on, there were only 46% that were actually privacy breaches. The rest were information breaches. So in terms of your numbers, I just want to make sure that's what that—

Mr. Mathieu Ravignat: Were all of those 46% of cases reported to the Privacy Commissioner?

Ms. Susan Gardner-Barclay: No. There's a protocol from Treasury Board that gives departments guidance on which cases should be reported to the Privacy Commissioner. It covers a fairly detailed risk assessment. Departments are asked to look at the sensitivity of the information that was disclosed. Is it, for example, financial or medical information? Departments are asked to make an assessment of the risk of identity theft or fraud as a result of the loss. Departments are asked to assess the potential to cause harm to the individual, for example, to the individual's reputation, their career—

Mr. Mathieu Ravignat: One per cent seems pretty low. In regard to those guidelines that you're following in order to not report some of these cases to the Privacy Commissioner, can you tell me a little bit more about that? Why is it there were so many that you decided not to report to the Privacy Commissioner, using those criteria? Was there one main reason or...?

Ms. Susan Gardner-Barclay: We are guided by the outcome of our risk assessment. If the risk assessment indicates that there is a reasonable chance of harm to the individual, then we will report to the OPC. In that timeframe, we reported 479 cases.

Mr. Mathieu Ravignat: Is that decision completely internal? Is the risk assessment completely internal, or is there an external peer review process to say, “Yes, you're on the right track; these cases shouldn't be reported to the Privacy Commissioner”?

Ms. Susan Gardner-Barclay: It is internal, but it is done in two different places in the agency. Ms. Brown's security and internal affairs division does the initial assessment, and then it is reviewed for quality by a separate shop in a separate branch in our ATIP organization, which has responsibility and close relations with the Privacy Commissioner to ensure that our assessments are, in fact, of the highest quality.

Mr. Mathieu Ravignat: Does Treasury Board then validate it? Is there a validation process?

Ms. Helen Brown: No, my understanding is that just recently Treasury Board has put in a framework for us to report to them, but up until this time, it's been the OPC that we deal with on these matters.

Ms. Susan Gardner-Barclay: The Treasury Board has asked that by next year all departments report privacy breaches to them as well as to the OPC, so that system is coming into place.

Mr. Mathieu Ravignat: Did the Privacy Commissioner, once she was aware of the breach and of the percentage that you reported to her, ask for any additional information?

● (1150)

Ms. Helen Brown: When you talk about whether it's an internal process, what I can say is that we did review our risk assessment tool that we use with the Office of the Privacy Commissioner to make sure it follows the spirit of the guidelines that come from Treasury Board.

I also want to clarify that there are two things that we assess. One is whether to advise the taxpayer, and one is whether to advise the OPC. There are two separate things going on in the area of your question.

Mr. Mathieu Ravignat: In regard to an order paper question from my colleague, Charlie Angus, he asked you to give statistics on how many privacy breaches there were between 2006 and 2012, but he didn't get a response from you. I was wondering why that would be. Is it that you don't collect this data, or that it isn't available?

Ms. Susan Gardner-Barclay: I'm sure Ms. Brown will want to add detail to my answer, but that is correct.

At the time, the CRA was certainly monitoring privacy breaches, but we were doing it by monitoring and tracking centrally the number of investigations. At the time that question was asked, we had not centrally started to record within each investigation how many breaches had occurred and how many individuals had been affected.

Mr. Angus' question asked for that specific detail. In order to be able to produce it, we would have had to go back through many years of reports and manually cull that information from those reports.

With Mr. Angus' guidance, we've changed our process so that we now are able to centrally track both individuals and numbers of breaches within each investigation.

The Chair: Thank you.

I'm afraid that concludes your time, Mr. Ravignat.

Next, for the Conservatives, is Ms. Tilly O'Neill Gordon.

Mrs. Tilly O'Neill Gordon (Miramichi, CPC): I want to thank the witnesses for being with us today. You bring us great information on things to think about. I also want to thank you for all you do to ensure the safeguards that are in place to protect Canadians' personal info, and in turn, reduce the risk of identity theft. Of course, for all of us that's a very important aspect and a very important idea to think about.

At the same time, I was going to say for the CRA, we all have a role to play in preventing identity theft. What roles do you see that consumers, businesses, banks, the federal government, the Privacy Commissioner have to play in preventing and combatting identify theft? Can you give us some ideas?

Ms. Susan Gardner-Barclay: Well, you're right, certainly the CRA views privacy—

Mrs. Tilly O'Neill Gordon: You guys are doing lots, so we should be handling something, too.

Ms. Susan Gardner-Barclay: We certainly view it as a shared responsibility.

With regard to what we ask Canadian taxpayers to do to protect the information that they send to us, we always ask them to make sure that they have verified that they are dealing with us, that whenever they're in doubt, they take advantage of our 1-800 numbers and call us to be sure that they're sending the information to the right people in the right way. We're quite involved with the Competition Bureau and financial literacy month, which is another area that we participate in. We do think it's important and helpful for Canadians to understand how their finances work and the kind of information they should be ensuring is kept secure.

Along those lines, a lot of it is around common sense, in some respects, absolutely. But we do have a significant amount of information on our website that helps people understand what the tax system is about and at which points they should be interacting with it, with very careful direction on how to do that so that they are, in fact, sharing only the information they should be sharing with us, and protecting it.

Mrs. Tilly O'Neill Gordon: Do you have something to add?

Ms. Helen Brown: I was just thinking about all the things that we do in CRA, and my colleague alluded to them in her opening remarks, about outreach to try to warn people of the risks to their privacy. On our website we give them tips on what to do to help guard against identity theft.

Mrs. Tilly O'Neill Gordon: The more and more we listen to witnesses talk about identity theft, the more I, as an individual, and anybody in my constituency, I would say, should come to realize how important it is that they keep their own information very confidential and work to prevent this identity theft, which can be on a rampage all the more with all this new technology, I suppose.

This question is for the Canadian Human Rights Commission. In January 2010, Bill S-4, An Act to amend the Criminal Code (identity theft and related misconduct), passed and added new Criminal Code offences that target the aspects of identity theft.

What impact did the introduction of these new offences have on affected organizations and government institutions in charge of law enforcement? Did that have any effect on them?

● (1155)

Mr. Philippe Dufresne: I'm not sure that we'd be best placed to answer that. From the standpoint of the Canadian Human Rights Commission, those new offences are not offences that come under our purview. They are not matters that people could come to us for in terms of complaints, so I'm not sure what the impact has been on other organizations on this.

Mrs. Tilly O'Neill Gordon: Okay.

Now, as we go forth in this study, do either of you recommend any particular aspects of this issue that the committee should really be focused on?

Mr. Philippe Dufresne: If I may, from the Human Rights Commission's perspective, we should keep a human rights lens on whatever measures we put forward, including measures to prevent and redress identity theft. From our standpoint, putting a human rights lens on policies, whatever they may be, is not in competition with the goals of those policies, but it will really, ultimately, strengthen the policies. That would be our broad recommendation on this.

The Chair: That concludes your time, I'm afraid. Thank you very much.

We're going to do one more round. Actually, we're going to do an NDP round, a Conservative round, and a Liberal round, and then conclude this part of our study. Then we'll be going into an in camera planning meeting for the rest of this session, colleagues.

We have for the NDP, Charmaine Borg.

You have five minutes, please, Charmaine.

[*Translation*]

Ms. Charmaine Borg: Thank you very much, Mr. Chair.

My first question is for Mr. Dufresne.

Do you believe the process for handling identity theft-related complaints is fair and effective? Could it lead to discrimination? Is the system adequate?

Mr. Philippe Dufresne: We didn't look at that specifically, so I would be reluctant to say one way or the other.

But we do believe that it's useful to ask that question for any process or approach. It's important to consider whether the process, which may have emerged from the best of intentions, has a negative impact on seniors, women or individuals with disabilities. And if it does, the solution is not simply to put an end to the measure automatically, but to determine whether it is necessary and whether the discriminatory impact can be reduced.

That's what we tried to do with our impact assessment tool. The idea isn't just to identify the practice as a barrier in principle, but to try to help organizations. It's not easy to achieve these objectives, but they do have to be achieved.

Ms. Charmaine Borg: Thank you very much.

My second question is for the CRA officials.

More and more Canadians are filing their tax returns online. Obviously, it's a digital world we're living in. Are the risks greater when taxpayers use the new software applications available to file their income tax return? If so, how can we advise Canadians of those risks and the way to safeguard against them?

[*English*]

Ms. Susan Gardner-Barclay: Again, this area is a little outside of our area of expertise. What I can tell you is that we have a very big recertification process for all of the software that is available through our site, commercial software, to file income tax and benefit returns. These cannot be certified by the CRA until they've met our very high security standards.

I can also tell you that with regard to our own systems and portals that are used by businesses, individuals, and representatives to deal with us on a variety of matters and access several services, including filing returns, we use the same high level of security that is used by Canadian financial institutions for online services. They are monitored at all times, obviously particularly during tax season, but we're very cognizant of the fact that security, the security of those portals, is instrumental to Canadians having confidence in sharing their information with us, so we have a very rigorous security system around the CRA system.

It essentially is a tiered system. It starts with Shared Services Canada. That has a number of security mechanisms around the outer layer. The next layer is CRA's own firewall, which is extremely strong. In the very rare instances where some kind of malware may get past that firewall, we have a second firewall that also bounces back any kind of malicious software or malicious attack. We have one of the strongest, if not the strongest, security regimes around our technological systems of any government department, for precisely the reasons you're talking about.

● (1200)

[*Translation*]

Ms. Charmaine Borg: Excellent. That's good to hear.

My last question may seem a bit odd.

Could you list all the pieces of personal information you have on a typical Canadian who files an income tax return every year?

[*English*]

Ms. Susan Gardner-Barclay: Well, that's...yes, we can—

Voices: Oh, oh!

Ms. Susan Gardner-Barclay: Obviously all of the information on a person's income tax and benefit return...so that would be the SIN, their income, and the credits they're applying for. To apply for some credits, you need to provide additional information. It could be medical information, if you're applying for a disability tax credit, for example.

For businesses, the general approach is the same. They must obviously provide business income. They must provide information on the GST and HST that they have collected on behalf of the government. If they are applying for credits, for example, business credits like the research and experimental review credit, they will have to provide information on the work they're doing in order to qualify for that credit.

It's very hard to summarize it in a way that's concise, but yes, we collect a significant amount of information. That's really only a taste of it.

[*Translation*]

Ms. Charmaine Borg: It's likely more than all the other departments.

Mrs. Susan Gardner-Barclay: Possibly, yes.

[*English*]

It's probably important to mention also that we do collect information on behalf of some provinces and territories as well, as a more streamlined approach, so we do have provincial information that we collect on their behalf too.

The Chair: Very good.

Thank you, Madam Borg.

Mr. Zimmer, for the Conservative Party.

Mr. Bob Zimmer (Prince George—Peace River, CPC): Thank you for appearing before the committee today.

Since we're talking about the economic impact, and correct me if I haven't heard the number, what is the average economic impact on a Canadian who has had their ID stolen, or on Canadians at large? Maybe the CHRC would have a better grasp of that. I'm sure it ranges from a small amount to a large amount, but what is the average impact financially?

Mr. Philippe Dufresne: Unfortunately, this is not information that we've collected, the impact on privacy.... We would look at the impacts on the human rights of Canadians of discrimination and so on. I can't provide that.

Mr. Bob Zimmer: The dollar value couldn't be quantified, essentially, from your—

Mr. Philippe Dufresne: It may be quantified, but it's not something that the Canadian Human Rights Commission would be quantifying.

Mr. Bob Zimmer: How about answering the same question from the CRA perspective? That would be just—

Ms. Susan Gardner-Barclay: Regrettably, the answer may be available, but the CRA would not track it.

Mr. Bob Zimmer: That's fine.

Since it's tax season, a lot of us use electronic means of filing our taxes, and I guess there are probably good programs and bad programs. I was just doing some searches on the web. Are you seeing that as potential fertile ground for people with identity theft motives, to somehow target free tax programs or that kind of thing? Have we seen that in Canada yet? I see it in other countries, but have we seen it in Canada yet?

Ms. Susan Gardner-Barclay: Again, it's outside our expertise, but we're not aware of any instance where we would have run across that.

I mentioned in response to a previous question that all of the commercial software that is made available on the CRA website has gone through an extremely rigorous authentication and certification program. We're absolutely confident that the software that's listed there works well with CRA systems and is secure and safe to use.

● (1205)

Mr. Bob Zimmer: So it would be key for Canadians to look at your list online to make sure they use services from that particular list. Good.

This is a question for both groups. What is the best way, and we can avoid the obvious, that Canadians can combat identity theft? That's a pretty broad question, but are there any particular programs that you would recommend? I know it's a bit beyond your purview as well, but do you have some recommendations for the average Canadian who might be reading what we're talking about here? What would you recommend to them as the best way of preventing identity theft from happening to them?

Let's start with Philippe, please.

Mr. Philippe Dufresne: What we would say, really, may be more directed to organizations that collect information, whether private, public, or government, and it would be to ensure that the methods used do not have an adverse effect on someone because of a prohibited ground, so they don't have an impact on seniors or persons with disabilities and so on. If there is, we must identify those impacts at the beginning stage when we're developing the measure, that we assess the measure, that we gather information to really monitor whether there is an impact, and what can we do to minimize it.

Mr. Bob Zimmer: Okay.

Yes, Helen.

Ms. Helen Brown: Canada Revenue Agency has a website about how to protect yourself against identity theft, which you might find of interest. It talks about things like never providing your personal information by Internet or e-mail. CRA never asks you to provide that type of information by e-mail. Anyway, there's a list: keep your access codes, your user IDs, and your PIN secret, keep your address current.... There are a bunch of things here and it talks about how to minimize your risk by protecting your SIN, immediately reporting lost or stolen credit cards, that sort of thing. We do have a reference that you might find useful.

Mr. Bob Zimmer: Sure.

I have one last question. I think my colleague across the way asked the question about the breaches that had occurred. You had said it had been incorrectly addressed mail or incorrectly received mail. I just wanted to highlight a specific thing that you had mentioned in what you had said. You said there was no personal information attached in those letters...some of them. What percentage of that group would you say would Canadians need to be worried about? Considering the breach as 100, how many would not have given personal information in that mail-out?

Ms. Helen Brown: If I understood your question, part of the answer is that of those almost 3,000 pieces of correspondence, 46% were considered to be privacy breaches and the rest were not considered to be privacy breaches. In terms of how many, I wasn't sure that—

Mr. Bob Zimmer: No, that's exactly what I was asking. So out of about 3,000, roughly half would be considered more serious, so literally.... And for those people, it's 1,600 too many, right? That's what we would say. I'm sure you would agree. But it's a fairly small number.

Ms. Susan Gardner-Barclay: Keep in mind that many of those pieces of correspondence were, in fact, ultimately recovered by the agency.

Mr. Bob Zimmer: Perfect. Thank you.

That's all I have.

The Chair: Thank you, Mr. Zimmer, your time has concluded.

Mr. Regan.

Hon. Geoff Regan: Mr. Chairman, I'm going to return to the question that I was beginning to ask before I was so rightly interrupted, and courteously interrupted, I must say, but it seems like an oxymoron, doesn't it? But it was of note because my time was obviously up.

Let me go back to the question of the breaches. When I asked about the processes you had in advance of last year to avoid them, you focused mainly on the breaches that were not misdirected mail. Let me refer to the 2,800 examples of misdirected mail. I guess the key question would be, what have you changed since January 1 of last year? That will really tell me both what it was and what it is now.

Ms. Helen Brown: I can come at your question a couple of different ways.

What we've done in the last couple of years is we've started to centrally manage the reporting of misdirected mail so that we are able to better manage it. When we do hear of cases of misdirected mail, we can contain it, we don't send any more mail to that address. We retrieve the mail in, as I said, 95% of the cases. We try to find the root cause of the misdirected mail so that we can correct it and reduce the risk of it happening again.

Hon. Geoff Regan: When you say that you retrieve 95%, I presume that the only way you become aware of misdirected mail is when someone receives it and notifies you. Is it fair to say that you really can't say for certain that it is 95% of all mail that is misdirected?

● (1210)

Ms. Helen Brown: You're correct. We can't say with certainty.

Hon. Geoff Regan: Just so I understand how this can happen, is it human error? Does a person put the letter in an envelope? Have you looked at the question of having that done electronically, or have you found that there are more errors with one versus the other?

Ms. Helen Brown: One of the benefits now that we've gone to centrally managing is we can actually track what the causes are.

For example, a range between 10% and 15% is because we didn't have the correct taxpayer address. Perhaps the taxpayers moved and didn't advise us. There's a certain percentage that are Canada Post errors of delivering it to the wrong place. There is a certain percentage of input errors: an employee receives a handwritten tax return and when they input it into the system, they put the numbers in backwards or something. We have some electronic or technical errors, and there are some double-stuffed envelopes.

We're tracking what the problems are and we're trying to rectify anywhere we can to reduce the volume of misdirected mail.

Hon. Geoff Regan: In terms of the times when a person puts the wrong document in the wrong envelope, let me go back to the question I asked about having that done by machine as opposed to humans. Is that a possibility, and have you a way to assess whether that would be more secure and have less of those problems?

Ms. Susan Gardner-Barclay: In fact, all of our print-to-mail operations are essentially automated now.

When you get something in a wrong envelope, it's usually a machine error. It usually means that a machine has picked up two pages instead of one, or somehow the flow between the envelope and the documents that are to go into it has been altered in some way within the machine. It's a machine or technical error.

We don't have, except in very rare instances, and again I'm not sure I could point to any, but it's very rare that we would be putting documents in envelopes by hand. We just deal with too much.

Hon. Geoff Regan: I obviously encourage you to keep working at that because people get very upset about it and I appreciate your being here today to talk about it.

Thank you.

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

If that concludes your questions, that does conclude this round of questioning, but I would like to take the prerogative of the chair to ask one question, or ask for clarification at least, on one thing that I believe I heard in testimony.

A recurring theme of the Privacy Commissioner has been that the public has a right to know if their information held by others has been compromised. Is it in fact the policy or the practice of the CRA that they do proactively inform any citizen whose privacy may have been infringed upon?

Ms. Susan Gardner-Barclay: In this instance we do follow Treasury Board of Canada policy.

We spoke earlier about the risk assessment that is undertaken to determine the degree of the breach and its impact on an individual, and that includes whether there is potential for identity fraud. It covers three separate areas, including what kind of harm might be possible with regard to the individual whose information has been lost, including impact on reputation or career or health or safety. It's quite a detailed assessment that we go through. It is in accordance with Treasury Board of Canada policies. When we do that assessment and the outcome recommends that we inform the Privacy Commissioner, then we do that and we also inform the individual.

The Chair: Just so I'm clear, in a case like Madam Borg cited, that happened to her, the envelope she opened contained somebody else's information, would that other person have been notified by you that their information was accidentally sent to another party?

Ms. Susan Gardner-Barclay: I can't speak about specific instances, but the informing of an individual would be dependent on the outcome of the risk assessment that we did based on the criteria in that fact case.

The Chair: Okay, very good. Thank you very much, then.

Thank you to our panellists from the Canadian Human Rights Commission and the Canada Revenue Agency.

We're going to suspend the meeting briefly and go into an in camera planning session, so anyone who is not authorized to be in the room can take their leave at this time.

Thank you very much for your testimony.

[*Proceedings continue in camera*]