HANSARD

NOVA SCOTIA HOUSE OF ASSEMBLY

COMMITTEE

ON

PUBLIC ACCOUNTS

Wednesday, February 27, 2019

Legislative Chamber

Investigation Report IR19-01:
Department of Internal Services
Freedom of Information Access (FOIA) Website

Printed and Published by Nova Scotia Hansard Reporting Services

Public Accounts Committee

Eddie Orrell (Chair)
Gordon Wilson (Vice-Chair)
Ben Jessome
Suzanne Lohnes-Croft
Brendan Maguire
Hugh MacKay
Tim Halman
Lisa Roberts
Susan Leblanc

[Brendan Maguire was replaced by Hon. Zach Churchill.]

In Attendance:

Kim Langille,
Legislative Committee Clerk

Gordon Hebb,
Chief Legislative Counsel

Karen Kinley,
Legislative Counsel

Andrew Atherton,
Assistant Auditor General

WITNESSES

Office of the Information & Privacy Commissioner

Catherine Tully,
Information & Privacy Commissioner

Janet Burt-Gerrans,
Senior Investigator

House of Assembly
Nova Scotia

HALIFAX, WEDNESDAY, FEBRUARY 27, 2019

STANDING COMMITTEE ON PUBLIC ACCOUNTS

9:00 A.M.

CHAIRMAN
Eddie Orrell

VICE-CHAIRMAN
Gordon Wilson

THE CHAIR: Order, please. I'd like to call this meeting of the Public Accounts Committee to order. Before we begin our meeting today, I'd like to remind those in attendance to place their phones on silent or vibrate. I'll now ask committee members to introduce themselves.

[The committee members introduced themselves.]

THE CHAIR: Thank you. On today's agenda, we have the Information and Privacy Commissioner of Nova Scotia with us to discuss the report of the office regarding the Department of Internal Services Freedom of Information Access website. I'd ask the witnesses to now introduce themselves, please.

[The witnesses introduced themselves.]

THE CHAIR: Thank you. If you have any opening remarks you can make them now, please.

CATHERINE TULLY: Thank you for the invitation to appear before you today. I appreciate your interest in the work of my office. As Nova Scotia's Information and Privacy Commissioner, I am tasked with providing impartial oversight of government's compliance with our access and privacy laws.

Nova Scotians have entrusted government departments with significant amounts of personal information. Governments need personal information to deliver services to the public, but in collecting our personal information, government departments have a duty to protect our privacy.

The standard that the department was judged by in this investigation was a very basic one: Did the department have reasonable security in place? Our investigation revealed that the security was not reasonable.

My message today is simple. We are at a crossroads in terms of privacy protection in this province. If we continue to follow the path that lead to this investigation, without question more breaches will occur.

I made two sets of recommendations in this investigation report - one set to the department and another to the Premier and the ministers responsible for our privacy laws. The minister has accepted the recommendations I made to the department. So why am I still worried? What more is needed?

I made recommendations to modernize our outdated privacy laws in 2017 and I repeated many of them again in my letter to the Premier and the ministers responsible in my letter last month. Our law, the Freedom of Information and Protection of Privacy Act, was written in 1993. In 1993, there were 130 websites. Now there are more than a billion. Google was not even founded until 1998, and Facebook wasn't created until 2004.

We live in a world of big data analytics, innovation and online services. Businesses and governments want to take advantage of the digital age. The Freedom of Information portal breach is an example of what happens when governments try to deliver innovative services without robust safeguards that a modern privacy law requires. Our privacy law is obsolete. It lacks essential features found in numerous privacy laws from Saskatchewan to Newfoundland and Labrador to Europe.

So what's missing from our laws? Here are a few examples. First, there's no mandatory requirements to prevent privacy breaches. There is no requirement the government conduct risk assessments for new projects and programs to ensure that they identify and mitigate privacy risks before pushing go. There is no requirement that government consult the privacy oversight body when sensitive personal information may be at risk.

A second piece missing is, there is a lack of consequences for failing to abide by privacy standards. There are no meaningful offence provisions for individuals who engage in behavior that result in a privacy breach, and there are no consequences if, for example, a public body fails to follow the recommendations of the Privacy Commissioner.

Third, there is a lack of basic citizen rights. There is no right to notification when a privacy breach occurs. Currently, government employees decide if and when they notify citizens and my office of a breach.

Modern privacy laws such as Europe's General Data Protection Regulation (GDPR), which you may have heard of, set meaningful standards with serious consequences. Governments are required to build privacy into their projects before launch, mandatory risk assessments, mandatory consultations with privacy commissioners, mandatory contract terms with service providers. Citizens are given meaningful rights - the right to be informed of what's collected, why it's collected, how long it will be kept, the right to notification of privacy breaches, and there are meaningful oversight powers, including order-making power and significant fines for non-compliance - up to 20 million euros under GDPR.

Serious and meaningful privacy rights and rules support a culture of respect for privacy in business and in government. Nova Scotia does not have this culture or these standards. We have a 20th Century law and 21st Century privacy challenges.

While citizens in other provinces and around the world enjoy meaningful privacy rights, Nova Scotians have been left behind to wonder when the next breach will occur and, if it does, will they even care about it.

So what next? I've made recommendations to modernize our law. There are many good examples of modern privacy laws available to Nova Scotia. Every recommendation I've made is based on the experience of other jurisdictions. These are well-travelled and proven standards.

Leadership in this area requires the creativity and courage to innovate in a way that will not only make Nova Scotia a leader in data and technology, but also in privacy rights and citizen trust. I would be happy to take your questions.

THE CHAIR: Thank you very much, Ms. Tully. We'll open the floor now to questions, beginning with the PC caucus and Mr. Halman.

TIM HALMAN: I want to thank you for your opening remarks. What you've indicated certainly has got me thinking - in particular, a statement you just made that we have 20th century laws and 21st century privacy challenges. That got me thinking. I'm curious if the Privacy Commissioner was an independent officer of the Legislature, how would that impact you doing your job? Would it improve transparency? Would things be done a bit differently in terms of oversight?

CATHERINE TULLY: There are two significances from my perspective in being an officer of the Legislature. One is the independence it brings from any government department over whom I have oversight. It would then allow me to report directly to a

committee of the Legislature so that the information that I know is regularly communicated to MLAs for you to be able to do your work and have that information.

The other that is usually associated with that would be an order-making power, so that instead of just having recommendation-making power, my recommendations would have more power in terms of influencing change.

TIM HALMAN: Am I correct in saying we could produce better public policy if the Privacy Commissioner was an independent officer of the Legislature? Am I correct in saying that?

CATHERINE TULLY: I believe so, I would certainly be providing information that would support your work.

TIM HALMAN: By way of example, if you had the independence of the office to release, for example, the Bay Ferries figures that you said should be released - in your opinion, do you think there would be harm to the ferry service or any other business wanting to do business in Nova Scotia? What do you think the harm or consequence of that would be?

CATHERINE TULLY: If I had order-making power, I would have said to the government departments, I order you to disclose this. That wouldn't be the end - the government would certainly have the right to appeal to a court. In the end, it would be up to the government department to disclose. My office would never be the office disclosing the information, that's very important. I'm the decision maker, but ultimately, they hold the data and they would be the ones to comply with the order.

The second part of your question was, would there be any harm? That decision makes it clear that the evidence did not support that there would be harm of the type alleged by the third party, from the disclosure.

TIM HALMAN: I'd like to get into the specifics of your report, and I want to thank you for the report, it was very detailed. On Page 6 you stated that, "More than 600 documents containing personal information were downloaded onto an unknown computer and have not yet been recovered or secured." Do you know if these documents have been recovered or secured yet?

CATHERINE TULLY: We've had some ongoing conversations with the Atlantic School of Theology, but we have not been informed yet that these documents have been secured. As far as we know, they have not.

TIM HALMAN: Has the Atlantic School of Theology indicated a timeline as to when they'll get back to you as to the number of breaches and so forth? Is there a timeline attached to that?

CATHERINE TULLY: The evidence we have so far is that the school doesn't actually have the documents. The evidence we had so far was that it's actually downloaded onto an individual's computer. However, the school is conducting further investigation to dig a little deeper to make sure that that's indeed the case. There is no timeline.

Ultimately this report, it's really the department's responsibility to follow up with the school and see what more they can do to find these documents, if that's possible.

TIM HALMAN: Would you happen to know the range of material in question here that was breached by the Atlantic School of Theology?

CATHERINE TULLY: What we know is that it's 600 documents, and it's responses to access to information requests, which means it could be all kinds of things. It could be foster child files. Everything in the 600 has some sort of personal information attached to it. It isn't the stuff that was publicly disclosed. It ranges from highly sensitive - medical information, social insurance numbers, history of childhood sexual abuse - or it could be something less serious than that.

TIM HALMAN: These are very, very sensitive topics. These are very sensitive pieces of information for the residents of Nova Scotia. Am I correct in saying that the 600-plus documents - that figure hasn't changed as far as you know, in terms of what was breached?

CATHERINE TULLY: That's correct. In the report, there's a description of the numbers of documents. We created that chart. Actually, Janet Burt-Gerrans sitting with me here was the lead investigator. At Page 34, we looked at the audit documents that the government provided to us, and we did some math to figure out how much is personal information or not. According to our review of the documents, 600 is how many documents with personal information were downloaded by this individual.

TIM HALMAN: At this stage, has everyone been notified of these breaches? Could you give us an update on that?

CATHERINE TULLY: We haven't received an update yet from the department. We have a meeting planned - I think it's in two weeks - where they're going to give us an update on their implementation on the recommendations, one of which was to go through these documents and identify further individuals who require notification.

TIM HALMAN: Do you think everyone should have been notified by this point, given the nature and sensitivity of this information?

CATHERINE TULLY: To be clear, the department notified all of the FOI applicants. The people who made the requests for information did get notification, and they

got that notification in a very timely way. Who they didn't notify are people whose personal information is inside the documents.

I make a request for records related to my childhood if I'm a foster child - in those documents are perhaps my birth parents, foster parents, and witnesses. There are other people identified - maybe my siblings - in the records. I would have gotten notice, but what I said in this report is that they need to read those 600 records and identify others who are identifiable who should also receive notice.

Do I think they should have done that from the outset? Yes, I do, which is why I recommended that they do it now.

TIM HALMAN: Given the pace of where this is going, I have grave concerns. Given the nature and sensitivity of this information, I think Nova Scotians would want to be informed if their information was breached. Is it fair to say that perhaps some will never know that their private information was breached, based on the pace that we're going at here? Is that a fair statement?

CATHERINE TULLY: It's fair for a couple of reasons. One is that the audit records for the database in question, the FOI website, the first four months that that website was up and running, the audit records for that time period were deleted in accordance with the retention period. During those four months, it's possible somebody accessed the records, and we'll never know.

The second group of people who will never know is - in order to identify an unauthorized access, they had to look for patterns in the audit records. What they did was, government folks looked for somebody who was looking at a whole bunch of the records or repeatedly going back. That gave you a sense that perhaps it wasn't authorized. It was through looking at patterns that they identified unauthorized accesses, but there could have been individuals who accidentally or one-off went into a record they weren't entitled to look at. So there is definitely a group of Nova Scotians who potentially could have been affected, and we'll never know.

TIM HALMAN: This is alarming. If I have understood you correctly, that some will never know, especially in light of your very upfront comments that security was not reasonable and that government has a duty to protect the privacy of citizens. That has always been the case, but certainly in the digital age, it is imperative. It is alarming to hear that some may never know that their privacy was breached through this incident. I'm curious as to whether or not you're aware of any directions or communications from the police on how the Department of Internal Services should proceed in the days following the discovery of the breach.

[9:15 a.m.]

CATHERINE TULLY: We interviewed several of the police officers who were involved in the investigation. They weren't in a position to direct the public bodies, and they were clear in their evidence to us that they didn't see that as their role. They were prepared to take whatever steps were needed, depending on what the government did.

I think this might be in reference to the potential delay or not in notification. They were clear that they didn't recommend a delay in notification, but they recognized the benefits of a delay in terms of being able to potentially seize the equipment that had the records on it without the person being tipped off to the fact that the investigation was ongoing.

TIM HALMAN: Going into the report - on Page 6.8, you stated that you wrote to the Premier on the topic of recommendations that you made two years ago. I'm curious as to how the Premier responded to your first letter regarding the recommendations you made at that time.

CATHERINE TULLY: The first recommendations were the Accountability for the Digital Age, which I mailed to a variety of people, including the Premier. I did not hear back directly from the Premier. About a year later, I followed up with the Deputy to the Premier, who indicated that they had received the report and were considering it.

TIM HALMAN: Did they indicate any specifics at all as to how they were following up on your recommendations?

CATHERINE TULLY: They did not.

TIM HALMAN: So essentially it was the same message - we're basically looking into this, no specifics whatsoever. Am I correct in saying that?

CATHERINE TULLY: That's correct.

TIM HALMAN: Do you feel confident, with the way the Premier responded to your letter, that these recommendations of yours will in any way be made complete? Am I correct in saying there was no evidence in that letter saying that we're going to follow up on these things?

CATHERINE TULLY: Sorry, I did get a letter in response to my most recent correspondence from the Attorney General indicating that they're studying the recommendations. I am optimistic by nature.

I'm also heartened by the fact that this committee asked me to appear today. You're all MLAs. The fact that I'm recommending a change in law - this is completely within the work that you do, and I'm encouraging you to consider these recommendations.

Am I optimistic? As I said, we're at a crossroads. We have to have a change. We cannot stay with this law. That is my opinion. I've been in the privacy business for 20 years. This law will not do. It will not protect Nova Scotians. We need to move forward. Government needs to use this data. It needs to use these systems, but we need to have a modern privacy law. Europe is miles ahead of us. Why would we want this? Why would we want less for Nova Scotians than everybody else has?

I think people understand that. I think that the potential is here. I know that it takes a lot of doing to change an access or privacy law. Every province struggles with these issues. But the time has come and I'm doing my best in my role to make sure that you have that information as you consider this.

TIM HALMAN: Do you think the Premier and the minister are taking this matter seriously enough?

CATHERINE TULLY: By "the minister," you mean the Minister of Internal Services?

TIM HALMAN: Yes.

CATHERINE TULLY: I do actually think the Minister of Internal Services is taking it seriously. I had a meeting with her. She expressed her deep concern about what had happened and her commitment to working towards meaningful change, and I take her at her word. I do intend to follow up with her as we have these meetings and work on the recommendations directed at the department.

I don't think that will be enough to make the change we need to make to secure the privacy of Nova Scotians, but I think it's very important.

TIM HALMAN: With respect to that, do you think it's reasonable that, if they're taking it seriously, there should be clear indications and certain clear changes in behaviour? If the very people who oversaw this breach are now tasked with the responsibility of fixing this breach, does that strike you as reasonable? Shouldn't there be a shakeup or a change to ensure that these changes are implemented? Do you think that's a reasonable statement?

CATHERINE TULLY: My report points out that there are serious culture issues, we saw concerns. I have to be clear, these are public servants who have a commitment to public service. They meant to do the right thing. It fell far short.

Are they capable of doing the right thing? I think they are. I do think that changing culture is a huge challenge. Like I said, I'm optimistic that change can occur. I do think it will be quite a challenge.

TIM HALMAN: You've certainly indicated that you feel your powers should be extended and further enhanced. I'm curious, what was the Premier's response to that, to you, your call that there should be more powers for your office to be extended and enhanced? What was the response to that?

CATHERINE TULLY: I haven't heard directly from the Premier on that topic, I've only heard media reports.

TIM HALMAN: Thank you. Time, Mr. Chair?

THE CHAIR: About four minutes.

TIM HALMAN: In the report on Page 18, "[58] The FOIA website Project Charter identifies the project as having ambitious time frames. It lists as a project constraint 'very tight timelines as the project needs to be approved, executed and implemented in 2.5 months.'"

Is it fair to say that these timelines resulted in, I guess, not proper levels of due diligence?

CATHERINE TULLY: They certainly contributed to that, absolutely.

TIM HALMAN: Can you give some specific examples where you observed that?

CATHERINE TULLY: What the report highlights is that in the project management there weren't proper risk assessments done, there were not proper security assessments done, that the privacy impact assessment wasn't thorough enough.

Our observation is that because they were rushed, I think it also contributed to relying on that initial low-risk assessment of a project that was never low risk, so it created pressure to just get things done. That meant they didn't take the time to do a thorough analysis. There were a number of points along the way they could have discovered the risks but did not.

TIM HALMAN: That's alarming. Certainly, something as important as this you certainly want to see due diligence, you want to see quality.

In your investigation, I'm curious, what reason do you think the minister and the department had as a priority to justify meeting this tight deadline? I'm curious if you spoke

with any witnesses from the department on how they felt about that. Where was this pressure coming from?

CATHERINE TULLY: We asked a lot of questions around that to try to understand better because it was their own documents that revealed to us that there was this tight timeline. We were not able to discover what the source of that pressure was. Witnesses either said they didn't remember or didn't know.

TIM HALMAN: Later in the report, a senior executive of the department was quoted as stating to ". . . (send her the document and invite her for a demo) as just FYI: there is no possibility to accommodate any change she may request." Do you consider this response more or less showing a position of disinterest for security concerns, or simply someone who is rushed by a deadline?

CATHERINE TULLY: I think they were rushed by a deadline. I can say I knew they weren't really interested in what I had to say because they were showing me the system two weeks before it was going to go live. Realistically, if I had a serious concern or any concern, it was very unlikely to affect how the system would be implemented. I understood that at the time, but of course, I still went to see the system.

TIM HALMAN: How did they respond when you suggested that to them? What was the response?

CATHERINE TULLY: When I said they needed a security threat and risk assessment?

TIM HALMAN: Yes.

CATHERINE TULLY: They said they had done a thorough privacy-impact assessment.

TIM HALMAN: Wow, okay. It seems like this behaviour wasn't unique. It seems that the Architecture Review Board provided statements to the minister that there were risks associated with the lack of website vulnerability scanning. Do you think this behaviour was much like how they had treated your recommendations after seeing the demo? Do you think this was a situation of disregard for security concerns and risk, or simply a stressed-out department trying to finish a product, regardless of its final form?

CATHERINE TULLY: The evidence we had from a number of witnesses was that security concerns were often seen as a barrier to progress. This is part of the culture that really concerns me - that, and the individual who told us that he was ridiculed for raising privacy issues.

So where these things are seen as a barrier, I think it forces individuals to maybe downplay risks when instead, if we had a robust privacy and security-risk assessment and mitigation process, they'd be "Let's figure this out. What's the problem? That's the problem? How do we fix it? That's how we fix it. Okay, let's go."

That's what we should be doing, not "I guess it's not that bad. Let's just keep going and hope for the best." We need a different approach.

THE CHAIR: Thank you. We'll now move to the NDP caucus and Ms. Roberts.

LISA ROBERTS: I'm going to start by asking you to talk a little bit more about this privacy and security regime in Europe, which is miles ahead of us. When you say that there are no consequences here with our existing framework set by the legislation, and also no obligation to mitigate and prevent privacy breaches, can you contrast that with what does exist in that better regime? Who would suffer the consequences? Against whom would those significant fines, for example, be applied?

CATHERINE TULLY: For the most part, the fines so far have been against businesses that are also subject to the GDPR. Governments are subject to it too, with some exceptions for certain types of government work.

What I'm recommending here - and I used the 20 million euros just to give you a sense of how seriously privacy is taken in Europe. One of the things that we would typically have in a Canadian law is offence provisions, so that where individuals such as snoopers - who we've all heard about - are caught, there are offences that can result in fines and even jail time.

Other jurisdictions have prosecuted individuals in Canada for this kind of activity, and it creates a seriousness about the nature of the offences and the importance of privacy.

LISA ROBERTS: It's interesting - you were called in to start looking at this situation right at around the same time, but a couple days after the police were called in. It seemed like there was a recognition of seriousness in terms of the police response, and yet the effort was oriented towards the person who stumbled on the breach, as opposed to the source of the vulnerability, which was within the government itself.

Do you have any thoughts on how things rolled out and how this issue was framed, at least initially to the public, as being a case of a breach? You imagine a breach happening over a big strong fortified wall, and in fact, we didn't have a big strong fortified wall at all.

CATHERINE TULLY: The investigation established that this was a well-known vulnerability - one that has been on the published top-10 list for 10 years for this type of website. I think it did take some time for the department to appreciate that the nature of the

problem lay in project management, security-risk assessment, privacy-impact assessment - failures in those processes.

Initially, they characterized it in a different way, but I would say that in terms of their response - and I think you're asking a bit about their response - they called the police first. I'm 100 per cent okay with that in the circumstance. What you initially want to do and the best thing to do with a privacy breach is, can you contain it? What can you do to contain it? There was a window of opportunity where maybe they could actually get the data back. Absolutely, that should be the focus - to try to get the data back.

They had no legal obligation to notify my office, but they did within a very short period of time, and they provided us with the information that they had at the time. So they took some initial very good steps in terms of managing the breach, but the circumstances that led to the breach were obviously as described in the report.

LISA ROBERTS: If I understand the timeline correctly - they took down the site on April 5th. They identified that the breach was a result of well-known vulnerabilities on April 12th. There was just those seven days between when they pulled down the site and when there was an understanding of, oh boy, this was us not doing our work. In between times, you had been contacted and the police had been contacted. But you feel that when the police were presented with the issue, they were presented with the best understanding that the government had at the time when they characterized it as a breach?

[9:30 a.m.]

CATHERINE TULLY: The day the breach was reported to them, it was reported as an ability to change the URL. That is a well-known vulnerability. The very first day, it's not that the government discovered it; it's that an employee of another government agency phoned them and told them about it. From the very first day, they understood how it worked.

Really, what I was saying is that even to this day, some people think that the problem is that somebody misused the website. I think at higher levels, there was an understanding as we did the investigation that there was a lot of what they did that contributed to this FOI website being live with this vulnerability.

I think you're concerned with what the department reported to the police to get them to investigate and how it was characterized. We interviewed a variety of witnesses, including the individual who reported the incident to the police. Our evaluation of his evidence is that he reported what he understood. He did not have a technical background. It was for the police then to figure out was it a crime or wasn't it. There was nobody in the department who was in a position to make that determination.

With the limited information that they had at the time, a massive download of the entire database, lots of personal information by one individual - they don't know the motivation, and he's using some sort of program to make this happen - it makes you think he has a bad motivation. It happened about a month before but didn't seem to have gone anywhere. In a small window of opportunity, maybe they can stop it before it gets spread everywhere.

As the report points out, they had three choices: try to get it back voluntarily, but they don't know who it is; call the police; or commence a civil action to try to get information from the service provider on the IP address and so forth, which takes too much time. They chose, I think, the one option they have. I make recommendations to put in our new law ways in which the powers at the department might be able to use to identify individuals who have gotten information in this way that they shouldn't, to try to do something short of the police action. At the time, they had very limited choices.

LISA ROBERTS: From speaking with people external to government who are interested in technology and engage in hacking of the most benevolent sort - people who enjoy working with computers and working with data and downloading data sets - it is an activity that is done not necessarily with malevolent ends by a variety of players. I think those citizens have expressed to me concerns about how someone - in this case we ended up knowing a 17-year-old or a 19-year-old boy had the force of the law come down on him in a way that, given how easy it was to access the information, must have been unanticipated to him when he was engaged in that activity.

I want to go back to the security, the lack of privacy risk assessment and risk assessment from the get-go. This one portal, this one website, was to accomplish two very, very different ends. As someone who worked for a long time as a journalist before I was involved in community work and then politics - back in the 1990s, I actually worked for a time with Canadian Journalists for Free Expression and helped support a campaign around access to information.

I wouldn't want us to characterize access to information as being something that is impossible to do well. That's one of my concerns as this story has unfolded - that we might walk away thinking, "See, government can't give us access to our public information because it's going to put our privacy at risk."

Can you speak to that and speak to the fact that it's not impossible - it's not even necessarily especially challenging to provide good access to information? It's just that this was a site that was also supposed to be protecting some of the most private and personal information that people were seeking to access about themselves, and somehow the government thought that one tool could be the way to share both public information with anyone and also private information with one person who deserved to have access to it.

CATHERINE TULLY: The investigation report - what we understood and determined with the evidence was that the storage base was the same. There are two purposes. One is public disclosure of public documents. It's a great idea - proactively disclosing FOI requests that have already been processed and have no personal information so that you don't have to make another request. It's a great idea. It promotes open government.

The second part of the design was that individuals who make access requests - instead of getting old-school paper, they get an email that says it's ready electronically. They get a link, they click on the link, and there's their document electronically. Great. Searchable. So it has two functions.

The problem was that all of the records for here and all of the records for here were in one storage database. It is very possible to design a storage base with these intermingled records, so long as you have authorities assigned to the records so that only people with the right authorities get to see the various records.

What happened was that that was not present in this database. This was the design flaw. Certainly it's possible to deliver this kind of service. It's just that this product wasn't designed to do that.

LISA ROBERTS: How do you wrap your mind around the fact that this was not contemplated as a significant risk or a significant design challenge from the outset of this project being undertaken? That's what I just can't quite wrap my mind around.

CATHERINE TULLY: They were very alive to this issue, to the fact that they needed to make sure that personal information was not accessible by the public. But because they didn't do a security threat and risk assessment, because they didn't do vulnerability and penetration testing, they didn't realize that it hadn't actually been designed to do that. They were assured by the vendor that it could do that. They worked very hard on a process where they flagged the records that would go up on the public site and they were very careful to have some checks and balances so that nothing got sent to that site that shouldn't be public.

So it's not that they weren't aware. They were, but the failures in the project management, the security assessments, and the privacy-impact assessment meant that the vendor's assertions about security and design were never tested. Had they been tested, not only would they have found this fault, they would have found the 28 other faults that the penetration-vulnerability testing that was done a few days after the breach was discovered - there were significant other vulnerabilities existing in that design.

LISA ROBERTS: You remind me of some of the conclusions of the Auditor General's Office - that it was the reliance on the vendor, the close relationship with the vendor, and the outsourcing of the public body's duty to protect the public interest that

contributed to this great vulnerability. There was a sense that the vendor was going to protect the public's privacy interests, instead of the government owning that piece.

Your recommendations to the Premier for changes in legislation - how would your recommendations address that and ensure that even in circumstances where we are relying on vendors to build and operate products for us, the government remains clear about what its obligations are and what cannot be outsourced to even a trusted vendor?

CATHERINE TULLY: I don't recommend that something cannot be outsourced. A trusted vendor - obviously you want to use a vendor that will deliver on what is supposed to be delivered.

What I would say from a privacy perspective, and what protects best, is our privacy-impact assessments properly done. I've recommended that they be made mandatory. Part of the privacy-impact assessment process is you do a security assessment, so you take what the vendor tells you and you test it: number one, "They say this. Is that true?" and number two, "Is it good enough?" That didn't happen here.

There's no reason not to use vendors, but the public body is always ultimately responsible. They need to impose those same responsibilities on the vendor through contract terms known as a privacy-protection schedule. Everything that you as a public body must do, you make sure you impose that as a contractual term on your vendor so that the public is protected.

We take advantage of their skill and expertise, but we test it and we check it. As public bodies, we are ultimately responsible to ensure that that data is protected.

LISA ROBERTS: As you said in your opening remarks, you have recommended that the province's privacy laws need immediate amendment. The Premier has said publicly that the government will not bring forward amendments to the FOIPOP Act, at least in the sitting that begins tomorrow, and that he believes that the system is working.

Your position on these issues is based on evidence gathered through multiple investigations, not just this case. Do you have any sense of what evidence the Premier is using to come to his conclusions about the situation?

CATHERINE TULLY: I do not.

LISA ROBERTS: Okay. You said that you've heard back from your most recent communication, which was January 10, 2019. Can you repeat for me - I think you may have already said it - what was the substance of the response to your letter of January 10, 2019?

CATHERINE TULLY: In essence, that they would undertake analysis of the recommendations.

LISA ROBERTS: How many times have you made essentially the same recommendations? When would it have been the earliest time that you would have made essentially the same recommendation around changes to the legislation?

CATHERINE TULLY: The details are in that 2017 report, but I've been talking about amending the authority of the Information and Privacy Commissioner in annual reports for a number of years - probably four years.

LISA ROBERTS: When you communicate with your colleagues across Canada, across other jurisdictions, is there another jurisdiction where the person in your role, with your responsibilities, is as unsupported and hampered by the legislative regime around your office?

CATHERINE TULLY: That's a difficult question. I think I interpret that as, are there other Information and Privacy Commissioners who have only recommendation-making power? Yes, there are.

In terms of how frequently recommendations are adopted or not adopted, when I started in this position five years ago, there was already some discussion of whether the commissioner should have order-making power or not. I said at the time, you know what, I want to wait and see. If I make recommendations and they are generally accepted, then I don't need order-making power. I wanted to take the time to see how things panned out.

It didn't take too long to realize that that recommendation-making power wasn't working very effectively. In some places it is. Municipalities are much more likely to accept recommendations. Agencies, boards, commissions, universities, and health custodians will accept recommendations far more frequently than government departments do.

I think there has also been a change across Canada and other jurisdictions, a realization that information and privacy legislation, the oversight agency, needs to have more authority to be effective. Newfoundland, for example, changed its laws a couple of years ago to a unique model, which I think would be very effective in Nova Scotia. It's still recommendation-making power, but the public bodies have to either follow the recommendations, or they must go to court and get permission not to. There's still court oversight, but the burden is now on the public body rather than on the public. The body has to object to the recommendation. That's more effective.

[9:45 a.m.]

My office would continue to be more of an informal accessible process, which I think would be good - less expensive in terms of not having to then have an adjudication unit and that sort of thing. It seems to me to be a good small jurisdiction solution, and it's one I discuss in the main report.

LISA ROBERTS: Thank you.

THE CHAIR: Order, please. That ends the time for the NDP caucus.

I wonder, Ms. Tully, if we could get a copy of your opening remarks so we could get a copy to give to each of the caucuses before we continue.

CATHERINE TULLY: I only have the one scribbled up.

THE CHAIR: That's okay if it's scribbled up. We can copy it if it's okay by you. The clerk will do it.

Thank you very much. We'll now open the questioning up to the Liberal caucus. Mr. Churchill.

HON. ZACH CHURCHILL: Thank you so much, Ms. Tully, for being here. I want to first register our appreciation for the work you did on the report on the security breach. I know I speak on behalf of the minister and the departments that responded directly to your recommendations when I express the appreciation from government to have some expertise provided in these matters.

Most of us are lay people in regard to digital security. That creates a high level of fear, so when experts provide feedback, it does help us act appropriately. I'm very pleased that the departments that were impacted by your recommendations have responded - mostly, I think, in favour of those recommendations.

My questions are more general in relation to the Act. Specifically, I do have some questions around Section 17(1), under the heading Exemptions. According to the Act, it states, "The head of a public body may refuse to disclose to an applicant information the disclosure of which could reasonably be expected to harm the financial or economic interests of a public body . . . or the ability of the Government to manage the economy . . ."

There's a follow-up, Section 21(1), under the heading Confidential information:

> "The head of a public body shall refuse to disclose to an applicant information

> (a) that would reveal
>
> > (i) trade secrets of a third party, or . . . technical information of a third party . . .
> >
> > or interfere significantly with the negotiating position of the third party."

I'm wondering what evaluations are conducted within the office in relation to these clauses, specifically around economic impacts before a recommendation is made?

CATHERINE TULLY: This would arise when somebody has filed an access request, and the government department responds by withholding information and saying that there would be harm to the economic interests of the government department and/or harm to the financial interests of a third party. Then the person who requested the information files an appeal to us. We have two parties before us and an appeal.

What then happens is that they each provide argument about why they think the information should be disclosed or not disclosed. When it comes to me, the law says that the burden of proof is on the government or the public body - which could be the government department - to prove that there would be harm to the public body within the meaning of Section 17 and within the meaning of Section 21, which is the harm to the third party. I ask the department to provide whatever evidence it has in support of its position. There's quite a lot of case law around what would meet that burden of proof when the test is reasonable expectation of harm. It is up to the government department or whatever public body to provide that evidence.

On the third-party harm, it's actually a three-part test. You read the first part of the test, but there are two other things that have to be proven. Sometimes what happens with a third party is that they get notice, and they're the ones who object to the disclosure. If that's the case, they bear the burden of proof, and they have to provide evidence of the nature of the information, financial or trade secret; that it was supplied in confidence; and that the harm as described in the Act could arise. Undue harm is what the law says.

So it's the parties that provide the evidence to us, which I evaluate against the legal test in the law.

ZACH CHURCHILL: In terms of your evaluation of the arguments that are presented, those are legal. Is there economic expertise in the office that assists you in evaluating the economic impacts of recommendations?

CATHERINE TULLY: To be honest, so far I've never been given evidence of an economic harm that would require any expertise.

ZACH CHURCHILL: So there is no expertise within your office to evaluate economic impacts in relation to recommendations that might fall under these clauses of the Act?

CATHERINE TULLY: My role is to evaluate the evidence against a legal test, much like a court would do. There are no economic experts in my office. They're legal experts and access-law experts.

ZACH CHURCHILL: So it's fair to say that the focus of the recommendations stemming from your office isn't on economic impacts or outcomes?

CATHERINE TULLY: They're on the evidence and the law.

ZACH CHURCHIL: In terms of interpreting these clauses of the Act and the economic impacts - I mean, the purpose of these clauses would be to not do anything that would jeopardize a commercial interest or a public or economic interest. What are the parameters that you believe we use to examine these particular clauses?

Specifically, are we only looking at an impact to one company, as an example, if a recommendation impacts one company, or do we evaluate the broader economic impacts as well, particularly lending investment, market confidence, these sorts of things? Are these facts that are evaluated in your office, or that should be evaluated according to the wording of the law?

CATHERINE TULLY: I evaluate whatever evidence is given to me. If the public body believes that some of the economic harm relates to that, I am completely open to hearing that. My job is to evaluate the evidence against the legal tests, which is what I do.

To be completely clear, the fundamental purpose of access law is to give the public access to government documents, but there are some other important interests that are also in the public interest. There is a public interest in protecting the economic interests of the province - I completely get that. I follow what the law says, the standard of evidence required as set out by the Supreme Court of Canada or, for example, on the third-party business exemption with that three-part test.

There is a long line of cases, including a Nova Scotia case that says, for example, that a negotiated provision in a contract isn't supplied. So there are three requirements - financial information supplied that causes the harm. There is a long line of cases that says, if it's a negotiated term in a contract, it's not supplied so that it can't be withheld under the third-party business. That's the Atlantic Highways case.

That's the sort of thing I do. I know what the law is. I ask for evidence. I weigh the evidence against the law, and I make a decision. I try in those reports to be really clear

about what evidence I had and why I decided what I decided - so that I am as transparent as possible in terms of the reasoning. So what's there is what I had.

ZACH CHURCHILL: I think we've established that, obviously, according to the law and your interpretation of it, the focus of your office is not to be preoccupied with the economic impacts. If that's the case, then who should be occupied with those factors in your dealings?

CATHERINE TULLY: I think my only answer is that the burden of proof is on the public body. If they believe they must withhold the information, they have to meet the legal test in Section 17. If they don't meet the legal test, the law says they must disclose it.

ZACH CHURCHILL: And the legal test is defined by case law in these matters?

CATHERINE TULLY: Case law in the terms of the section of the Act.

ZACH CHURCHILL: Without having economic expertise in the office when there are matters of economic disagreement, what is the process that's undergone through this to find out what the answers are and to mediate the differences of opinion on economic impacts.

CATHERINE TULLY: The main challenges you'll see when you read the cases is that I am not provided with evidence that supports the public body's position, so we never get to a point where there's a disagreement.

I am looking for evidence that supports the government's position. Sometimes I will say back to them, I have a question about this. I may follow up to try to get more information but as you read the decisions I've issued you'll see what it is that I get and it is so limited that I make my decision based on the law.

ZACH CHURCHILL: But just to be clear and make sure I understand, the burden of economic impact isn't on the privacy commissioner's office - it is on the public body, mainly the body? Is that how I am to read the Act then?

CATHERINE TULLY: The burden is on the public body to disclose the information. That's what the law says - they must disclose it unless a specific and limited exemption applies.

ZACH CHURCHILL: Which could be financial, economic, commercial impact?

CATHERINE TULLY: It could be, yes.

ZACH CHURCHILL: Thank you very much, I appreciate your time.

THE CHAIR: Thank you, Mr. Churchill. We'll now move to Mr. Wilson.

GORDON WILSON: Thank you very much, Mr. Chairman. Welcome and thank you. I also want to start off by echoing the same comments my colleague did. I understand you work very closely with the Auditor General's Office in moving this file forward. I really do appreciate and we do value and I do believe we did accept every one of your recommendations in regard to your report on the data breach.

Again, we're lay people out here. It has been quite an education for us. We've had the Auditor General before us, we have you and I believe in a couple of weeks' time, we have the department here to thoroughly discuss and flesh out what happened and how we can do better to make sure that it doesn't. Your comments around that are appreciated.

It's important to know that we do have oversight from your office, along with the Auditor General and the Ombudsman, we have several oversight people who do take their job seriously to protect our citizens and the spending of our monies properly.

For me it was an understanding when I started looking into the reports and how this investigation rolled out of how the dovetailing of the two, between the Auditor General and the privacy office worked. It's my understanding that the AG looks at controls whereas you would look at the protection of privacy and information.

Can you expand a little bit more maybe on what your involvement was and how it did dovetail with the Auditor General in this report?

CATHERINE TULLY: Yes. It's fairly unique for a privacy commissioner to work with an Auditor General although we did a little bit of it back in British Columbia when I was the assistant privacy commissioner there. Our role is strictly as set out in the Freedom of Information and Protection of Privacy Act and the other related Acts.

Our job was to assess whether or not the government was in compliance with a particular provision of the law relating to reasonable security. That's what we did, we tested their activity against that legal test of reasonable security.

We had to evaluate what happened that led to the breach and then we evaluated the steps taken after, both in terms of was that reasonable security in both events. The Auditor General has their own mandate.

What worked well was that just the circumstances of the breach lent itself to an evaluation of project management, contract management, which of course is in the area of expertise of the Auditor General. They also have security expertise which we took advantage of as we went through an analysis of what the cause of the breach was because it was very technical.

GORDON WILSON: At the recent appearance of the Auditor General, they provided us with a description of how he sets the audit parameters and the standards of practice they follow, et cetera. Perhaps you could give us an overview of your office and your roles and how you structured investigations such as this and that background and how that helped you better position your findings. Again, we get a lot of information from the AG on theirs. It would very interesting for you to give me that kind of a snapshot on yours.

[10:00 a.m.]

CATHERINE TULLY: So how we structure investigations?

GORDON WILSON: Yes.

CATHERINE TULLY: I have a very small office. There are seven people in my office - Janet Burt-Gerrans is our senior investigator. What we do when we have a breach report - maybe this is the best way to do it - if a public body reports a breach to us, there are two possible approaches we might take. The first is that we may just monitor, and ideally what we would like is that the public body or municipality does their own investigation, figures out what happened and reports back to us, and we then evaluate that to make sure they've done everything that needs doing to secure the data and meet the standards in the law.

In other circumstances, if I have reason to believe it's more serious or systemic, we may initiate an investigation which the law permits us to do. In this case, that's what we did. Once the breach was reported to us, it was clearly very significant and would affect a large number of people, and it occurred in the very unit responsible for leading privacy. All of those things indicated to me that it was an appropriate case to initiate an investigation, which we did.

We do an investigation plan where we outline the steps we're going to take, who we're going to interview, and what kind of information we need to gather in order to examine whether or not the public body has met the legal test that I described to you. Our focus is always on the law, on the evidence needed in order to establish if the public body did or didn't meet the requirements of the law.

GORDON WILSON: When was the breach reported to you, to your office?

CATHERINE TULLY: I believe it was on the Monday, four days after it was initially discovered.

GORDON WILSON: I believe it was found on a Friday, so it was that following Monday that it was reported to you.

CATHERINE TULLY: Yes.

GORDON WILSON: Okay, thank you. In your report, in Paragraph 25, you say that the website was an important step forward in facilitating access to information and made a significant contribution to transparency and open government in Nova Scotia. Can you explain how your investigation reached that conclusion?

CATHERINE TULLY: That was a description of the portal where people could access previously-released FOI requests. That was something I recommended to the government when I first arrived four or five years ago, and it is something that is in place in other jurisdictions. That's a great way to be open and transparent: don't make people make access requests for stuff you've already disclosed. Just put it up there. That is what I meant by that. It was a good step forward in terms of openness and transparency.

GORDON WILSON: Thank you. I'll turn my questioning over to my colleague.

THE CHAIR: Ms. Lohnes-Croft, with about three minutes.

SUZANNE LOHNES-CROFT: Thank you very much. I enjoyed your opening comments very much. They gave me a better picture of your work with respect to this file.

I'm curious with what's happening with the investigation at AST. What is the delay? Do you know what it is?

CATHERINE TULLY: I wouldn't say necessarily that there's a delay. What we've done in the recommendations is ask the department to follow up with AST to see if there are some steps that could be taken to see if anything further can be discovered about the identity of the individual. We were in contact with them very shortly after we issued the report to see if their efforts were ongoing.

They were co-operating and were planning, as I understand it, to work with the department. We have a plan to meet with the department in two weeks to get an update on what's happening. I expect and I hope that at that time we'll hear that some progress has been made.

SUZANNE LOHNES-CROFT: Are the police involved in this part of the investigation?

CATHERINE TULLY: No, they are not, not that I know of.

SUZANNE LOHNES-CROFT: So I'm taking that AST is the Atlantic School of Theology. I'm quite familiar with them. I've worked with some students there in the past.

A lot of research is done there. My first thoughts are that someone is doing research on something that would be a topic - to me, that would be the first point. They're Master's and Ph.D. students, pretty much, right?

CATHERINE TULLY: We don't know anything about the motivation of the individual who has downloaded these 600 documents, but it doesn't matter in terms of the protection of privacy. That person shouldn't have those documents. The department is responsible for securing them.

SUZANNE LOHNES-CROFT: Okay. I'll be interested to see what direction that goes.

The Auditor General made remarks earlier about the speed of containing the breach and the time that the department reacted quickly to the breach. Would you agree with that - that the timeline was done quite quickly once the breach was discovered?

CATHERINE TULLY: I do agree, yes.

SUZANNE LOHNES-CROFT: When you meet with the department next week, do you have certain expectations of what you will hear?

CATHERINE TULLY: All we have is the very high-level summary of the steps they were planning to take to implement, and we're looking forward to hearing them. I hope for much more detail in terms of with each recommendation, what exactly they are doing, what their timelines are, and being able to tell whether or not it's actually an implementation of the recommendation or not. That's what we're looking forward to.

THE CHAIR: The time has expired for the Liberal caucus. We'll now move back to the PC caucus - Mr. Halman.

TIM HALMAN: Thank you. I just want to delve into the line of questioning from the member for Yarmouth. Did government provide the data needed to keep the management fee private?

CATHERINE TULLY: This is in reference to the recent review report. The review report itself states exactly what evidence was provided. My conclusion was that the legal test was not met, the burden of proof was not met, so there was not adequate evidence.

TIM HALMAN: I'd like to delve back into the report. The report states that the privacy impact assessment is defined as a ". . . due diligence process that identifies and addresses potential privacy risks that may occur . . ." and a privacy impact assessment is a requirement for each government entity when it involves ". . . any new program or service, that involves the personal information."

From my understanding of the report, there were some mitigation strategies identified in the privacy impact assessment, but am I correct in saying that there was a failure by the minister and the department to take action? Am I correct in saying that?

CATHERINE TULLY: That's correct, yes.

TIM HALMAN: One of the statements you made in my first round of questioning is that it was expressed to you that in the department there seemed to be this notion that security concerns were an impediment or barrier to progress. That to me, wow, that's powerful - security concerns, a barrier to progress.

Do you consider this response or this feeling that was expressed to you more or less showing that there was a position of disinterest in security concerns, and basically individuals motivated by meeting a deadline, feeling constrained, and perhaps not necessarily paying attention to the details of the end result - the end goal was just, let's meet the deadline? Is that a correct statement?

CATHERINE TULLY: What the report says is that several witnesses - not just one - indicated that they felt what was communicated to them on occasion was that security was a barrier. Certainly, there are people there - and we did speak to people - they care deeply about security. They want to do a good job. They want to make sure that the proper assessments are done, but this investigation revealed that there are definitely circumstances when the work is simply not done.

TIM HALMAN: On Page 25 [98], you provide a bullet list of shortcomings in the privacy impact assessment process. Would you say these can all be linked back to the deadlines, the time constraints, and I suppose the stress that was imposed and maybe never made flexible by the minister and the department? Essentially, it comes back to the culture of the department. Is that a correct statement?

CATHERINE TULLY: I think it's more complicated than that. I think the culture is part of the problem. There was a lack of privacy expertise - better training on how to do a privacy impact assessment.

There was a thing the Auditor General spoke about at length, and that is that the initial assessment of low risk - I think it brought everybody's temperature down and they didn't have their "Spidey sense" on. They weren't paying attention to the details in the way they should have. I think it was a mixture of things that contributed to this.

TIM HALMAN: Was there any evidence of the minister or any senior civil servants trying to change that culture within your investigation? Did you come across that at all, trying to shake that culture up?

CATHERINE TULLY: I would say in response to this investigation, there is an awareness now. Certainly the minister indicated that she takes this investigation seriously and the implementation of the recommendations seriously. As I say, I'm looking forward to seeing what happens in terms of the implementation and further discussions with the minister as we go forward.

TIM HALMAN: In your report, you mention that there is a potential for litigation exposure for the department. Have you heard if this is a greater potential risk for the department, or that it seems that the department has essentially lucked out and avoided that risk?

CATHERINE TULLY: I haven't heard anything in terms of whether or not a class action of any kind has been initiated.

TIM HALMAN: I'm curious - compared to past experiences with other cases, maybe across Canada or in other jurisdictions, has a privacy breach of this magnitude resulted in resignations, a shake-up of a department, or other dismissals?

CATHERINE TULLY: I have been at this for 20 years and probably have investigated or managed hundreds of privacy breaches. I have never seen one quite like this, to be honest.

In the early days, a lot of times, departments were learning how to manage privacy. Mostly the most significant consequences occur when the breach is caused by wrong-doing by an employee, so it's not unusual for them to be fired as a result of their activities. I have seen that, individual employees.

I don't recall anything other than lots of policy changes, training, new processes. That's the sort of thing that typically comes from these investigations.

TIM HALMAN: I appreciate you saying that. Certainly it give us a sense of the scope of analysis you have done over the years with privacy breaches. Is it a correct statement to say that this is one that Nova Scotians should really pay attention to, this privacy breach? This should be a wake-up call. Is that a fair statement?

CATHERINE TULLY: I think that's a very fair statement, yes.

TIM HALMAN: Because it is perhaps a moment where we should all be paying attention, in your opinion, should there be consequences within that department for this privacy breach? My understanding at this stage, and please correct me if I'm wrong, is that the very individuals who oversaw this security breach, which you have indicated is of huge magnitude - should there be consequences? Can we entrust those who oversaw the security breach to now fix this problem?

CATHERINE TULLY: My role as the privacy commissioner and my goal in these investigations is to make useful, realistic, legal recommendations that, when implemented, will improve the situation. That's what I have tried to do. I believe that the recommendations that I have made - if they're thoroughly implemented in a meaningful way - will make meaningful change both in the department and in terms of changing the law. Outside of that, I don't have any comment on that.

TIM HALMAN: We have certainly discussed the sort of lackadaisical attitude that existed in the department. There was an attitude that security was a barrier to progress, especially in light of the fact that in your opening remarks, where you indicated that we have a 20th century law within the context of the early 21st century. Are you confident that the mindset that existed in that department that led to this is no longer there?

CATHERINE TULLY: They say culture eats strategy for breakfast. No, it takes a lot to change a culture. It will take leadership. It will take a change in the law. It will take implementing these recommendations in a very thorough way in order to change the culture.

TIM HALMAN: You stated that, when asking witnesses in the department about the post-incident review and what were the lessons learned - you mentioned the bullet list provided on Page 39 in Point 158. I'm just curious, do you feel like the answers that were provided to you were genuine answers from the witnesses, or possibly talking points given to answer your questions on this topic, in order, perhaps, to keep that culture in place?

[10:15 a.m.]

CATHERINE TULLY: Our evaluation of the evidence was that it was very consistent that the witnesses for the most part were being genuine and were attempting to tell the truth.

TIM HALMAN: With all this in mind, the fact that no one has resigned - it's essentially the exact same group that is in place that oversaw the biggest security breach in Nova Scotia. You've indicated that you've analyzed many security breaches throughout Canada, and this is one to take note of. The fact that there are people within the ministry who possibly still don't understand the root causes of how this happened - also the fact that there is a negative culture in which critical and useful mechanisms like the Architecture Review Board were viewed as a roadblock.

Do you think the minister and the department are capable of getting us out of this mess and ensuring that Nova Scotians will never have to go through an experience like this again?

CATHERINE TULLY: I think yes. I have to believe they are capable of implementing these recommendations in a meaningful way and changing, because that's what needs to happen. Do I think it's enough? As I said, no. I do believe we need to have a change to the law as well, that both of these things have to happen to make meaningful change and to realistically move forward in the digital age.

What we need to do is build the value of privacy into our projects. We need to use technology, no question. We need to use big data, no question. But privacy is a value that

needs to be built in from the very beginning. It isn't a barrier. It's just a piece of the design of whatever it is you are working on. I think I've answered your question.

TIM HALMAN: We all agree that we have to move forward in the digital age. We need to update our laws. Do you find it alarming that the Premier doesn't seem to share those same concerns as you? I believe that if he did, we'd certainly be moving forward in that direction, but it seems that we're not. Do you find it alarming that that's not the case, that they are not taking these recommendations seriously?

CATHERINE TULLY: Well, as I said in my opening remarks, I do think we're at a crossroads. Change needs to happen. In my experience, based on the investigations, based on my 20 years, the time is now. The time was yesterday. We really need to modernize our privacy law.

Do I think it's urgent? I do think it's urgent. Do I think it's essential? I absolutely think it's essential.

THE CHAIR: Thank you, Mr. Halman. We'll now move to the NDP caucus and Ms. Leblanc.

SUSAN LEBLANC: Thank you for your comments so far. The Minister of Internal Services and the department have released an action plan in response to your recommendations. I'm wondering if you think the action plan, as it stands now, is sufficient to address your concerns? Is there anything missing from their response?

CATHERINE TULLY: We've reviewed it. It's too high level, in my opinion, to be able to clearly answer that, which is why we're having a meeting with them. We hope to get into significantly more detail to better understand exactly what the steps are that have been taken. Once we have that information, I'll be in a better position to say whether I think we're going to make significant progress or not.

SUSAN LEBLANC: Thank you. I hope that if you feel like maybe we won't be making significant progress, you'll let us know as soon as possible.

The same answer may stand for this question, but from what you've seen so far, I guess, do you think the plan is enough to restore the public's faith in the government's ability to protect our privacy?

CATHERINE TULLY: It's not enough for me. I need more detail.

SUSAN LEBLANC: The letter from the minister included in the 2018-19 business plan for the department states, "We take seriously our responsibility to make government information publicly accessible while balancing our duty to protect the personal

information of Nova Scotians. We will continue to deliver robust cybersecurity and information access and privacy programs to meet these obligations."

Given what we've heard today - and I'll quote you saying that when you conducted your investigation, in the department you heard that "security concerns were often seen as a barrier to progress", which I find deeply disturbing, and that an employee was ridiculed for bringing up privacy concerns. Given that and given the statement in this letter, would you agree with the minister's assessment that the department has been delivering robust cybersecurity and information and access and privacy programs?

CATHERINE TULLY: I think there is no question that in this case it did not. This was a serious failure of due diligence.

SUSAN LEBLANC: One of the findings in the Auditor General's Report on this incident is that an expert group within the department was not adequately consulted on potential risks or mitigation strategies. As we've discussed, many of the recommendations in your report were also included in a report the government received in 2017.

In your office's investigations, have there been other instances of issues arising because expert advice had not been solicited or appropriately addressed?

CATHERINE TULLY: There is no legal obligation to consult my office. What was unique in this case is that I did happen to be informed of the system just before it went live, and I did happen to say, you should do a security threat and risk assessment, and how do you know that individuals can't see each other's data on this website? So that's a fairly unique circumstance where I actually did give advice right before the system went live. In the other investigations, that circumstance didn't arise.

So one of the recommendations I make is that there should be a mandatory requirement to consult with us - not on every project because there are eight of us, but on projects that involve very sensitive personal information or integrated programs or activities where there are multiple databases being put together, things that would have a profound effect on the privacy of Nova Scotians. Then I say, come and see us early. What I say to government departments when they come to see me is that we're an independent eye. We're going to look at this and try to give you an indication of where we see risks or where we see mitigation strategies. It only makes your product better. There is no down side to coming and talking to us.

SUSAN LEBLANC: Based on that, my understanding now is that the law currently would not require, for instance, the Department of Health and Wellness and the Department of Internal Services when they are planning the One Person One Record system or the drug information system - they're not required to consult with you before putting those systems in place. Is that correct?

CATHERINE TULLY: That's correct.

SUSAN LEBLANC: That's deeply concerning because we already know from other Public Accounts Committee meetings and meetings of the Health Committee that the Auditor General has found that those systems have issues as well.

Given that, I would say that I as a member, although I'm not currently a member of the - given that the members of the public have a healthy amount of concern about all of this, especially given that we're going down the road to that very private information being online, it's clearly a key responsibility of the government to maintain a higher standard of care in its handling of Nova Scotia's private information. What should Nova Scotians expect the government do to protect their personal information?

CATHERINE TULLY: They should expect a modernized law to try to deal with these issues, and they should expect them to set the standards, such as the ones that I've set out. Although, the best approach to a new law would be to have some public consultation and ask the public what they want in a law. Ask the individuals who are affected by these breaches, privacy experts such as myself to provide information, but also people who use the Act - what do they want to see in the law? That would be the best law - one that we all contribute to that sets a standard that Nova Scotians expect.

SUSAN LEBLANC: Just going back to my first question about the One Person One Record, I didn't clarify. I asked if they had any legal obligation, but have you been consulted on the One Person One Record program?

CATHERINE TULLY: We are aware of it. We've asked questions about it, but we haven't been consulted on it, no.

SUSAN LEBLANC: In your report, Recommendation No. 5, the review of other technologies for security vulnerabilities, you made two recommendations. One is that "Within one year create an inventory of technology solutions, devices and applications that involve the use of personal information across government and rate the cyber security vulnerability and penetration risk based on modern standards of cyber security risk assessment." and, "Create a plan to mitigate cyber security vulnerabilities beginning with systems storing the most vulnerable personal information and/or having the highest risk vulnerabilities . . ." Then you say that by July 2nd of this year to provide your office with an update on the status of the plan.

I'm just wondering if there has been any interim status update or anything that you can speak about that.

CATHERINE TULLY: There hasn't been. This is really privacy 101. You can't protect privacy if you don't know what you have and where it is. Step number one is always to do an inventory. It's a huge amount of work if you haven't already done it. There may

be some inventories out there that are already in existence that can be adapted to this task. It's not clear to me exactly what's available. To me, that is one of the most important recommendations I've made, in terms of going forward.

The government needs to know what data it has, where it is, how sensitive it is, and if it's protected. I am looking forward to an update on exactly what steps are going to be taken.

SUSAN LEBLANC: Thank you. How much time do I have left?

THE CHAIR: Four minutes.

SUSAN LEBLANC: I'll actually hand it over to my colleague, Ms. Roberts.

THE CHAIR: Ms. Roberts.

LISA ROBERTS: It's interesting to think about the power of anecdotes, do they actually elucidate a bigger situation or don't they? I'm going to share an anecdote of a recent interaction in the health system. I was waiting quite some time for a specialist to look at my wrist and there was a computer screen there. I approached the computer screen and it was like oh, I was in the hospital for that; oh, I was in the hospital for that. Then I was like, I wasn't in the hospital for that, I don't remember that procedure, and there was another patient with whom I think I share a name - not a birthdate because I was able to look across and go, oh, that's a Lisa Roberts born on a different date and she has been in the hospital for these four procedures intermingled with my own health records.

It didn't have a lot of detail, but it had enough that I could sort of see what her health - why she had been engaged with the Nova Scotia Health Authority. What am I to make of that? What am I to make - is that a breach? Is that very concerning? Is that a situation that could be redressed, will be redressed with the One Person One Record? Or is that just kind of like yup, that's how it is, you know?

I mean there's also faxes that we know arrive at the wrong fax machine, et cetera, and obviously I'm not going to use that information in any way that is particularly concerning, but it's conceivable that I might have known that person but not known that health information.

CATHERINE TULLY: I'm unclear how you saw the screen.

LISA ROBERTS: I was waiting in a room for the specialist to come in and I think someone had retrieved my information, but they had retrieved my information in a way that both my health history but also this other person's health history with whom I shared a name were both displayed.

CATHERINE TULLY: You were in a private room and that was a screen intended for the specialist?

LISA ROBERTS: Yes, and I was just like waiting there for 20 minutes and I was like oh, what's that?

CATHERINE TULLY: Obviously, there's a few problems with that but there's no question that's a privacy breach. The screen shouldn't be up in a way that you could see it, so that's not reasonable security. It's an error that if your data is intermingled it's not clear - maybe it was, maybe it wasn't - without seeing what the record was.

You can ask for a copy of your own personal health information and find out if you're seeing somebody else's data. Did you mention it? No. You probably would have mentioned it in case it is an error because you certainly don't want the data intermingled.

Is this a potential problem in the health care system? Without question. It's an ongoing challenge. It's one of the reasons that these faxes get mis-sent and picklists are wrong. So many people share names so there has to be a number of identifying features to try to ensure that it's accurate.

There's no question as they design these system - that is one of the design goals: to make sure you properly identify the individual. But where data is intermingled, that's a significant problem, one that has to be addressed, and it's the responsibility of the health custodian to do so.

[10:30 a.m.]

LISA ROBERTS: We did have the opportunity to ask some questions about the One Person One Record project just last week or two weeks ago. I'm wondering if you had the opportunity to watch the proceedings of the Public Accounts Committee as we asked those questions. If so, what thoughts or recommendations do you have for us at this very important moment in that procurement process?

CATHERINE TULLY: I didn't see the proceedings that day. Without question, a project like this requires a very, very thorough privacy impact assessment. It needs to be at various stages. It needs to be at the idea stage, at the design stage, at the implementation stage, and then circle back to make sure that things happened that you said would happen so that you're identifying the risks early on, getting your design focused in the right direction, and then as you design it, figuring out where all the risks are. Are there any well-known design flaws that you need to be addressing? Do it as early as possible. It's way less expensive, it builds privacy in, and you get your work done.

That's what I would be expecting. I know that we have certainly raised the issue with the Department of Health and Wellness and hope that we will be getting more

information. We had a meeting yesterday trying to follow up on some of these projects. We will certainly be engaging with them, but they have no obligation to provide us with information, and they have no obligation to provide us with a privacy impact assessment. They may, or they may not.

THE CHAIR: Thank you very much. The time has expired for the NDP caucus. We'll now move on to the Liberal caucus. Mr. Churchill.

ZACH CHURCHILL: The member for Dartmouth East posed some very specific questions around the ferry that I'm probably better positioned to provide some insight on than the witness. Obviously, the concerns around our contract with the . . .

THE CHAIR: Order, please. Are you answering a question of Mr. Halman, or asking a question to Ms. Tully?

ZACH CHURCHILL: I'll be doing both, and they're connected.

THE CHAIR: The questions are not to the members of the committee. They're . . .

ZACH CHURCHILL: I'll bring the attention of the committee to an article that came out this week, "Investors Pull Out Of Development Plans In Yarmouth Over Ferry Rhetoric," specifically from the Progressive Conservatives. This was an investor who was looking at doing a major investment in the downtown, up to $6 million, I believe, in accommodations, which are desperately needed since the ferry had returned.

I'm very pleased, and I think Ms. Tully has rightfully pointed out that these sorts of preoccupations around not just the impacts to operator but market confidence, lending, investment, and property values are rightfully not a preoccupation of the privacy office. I'll table this for the committee as well. I guess I just want to register my surprise that this is not a preoccupation for the members of the Opposition Party. As is stated in the law itself around Freedom of Information and Protection of Privacy, these economic interests are deemed to be . . .

THE CHAIR: Is there a question, Mr. Churchill, or are you going to lecture somebody on what's going on in Yarmouth here? We're not here to lecture people on what's going on in Yarmouth. We're here to listen to questions and answers . . .

ZACH CHURCHILL: I'm sorry, I have a seat at the table here. I'm allowed to provide comments as the member did. The member spoke specifically to the ferry issue.

THE CHAIR: He asked a question to the Privacy Commissioner. So please . . .

ZACH CHURCHILL: For sure. Thank you.

As the Act rightfully points out, these matters of economic interest, of confidence, of lending, of investment, of job creation, and of growth are matters of preoccupation for government, and that's generally accepted in the public as well. That is something that the government takes very seriously. I do want to register my surprise that it isn't something that the member for Dartmouth East takes seriously or is concerned about.

My question to the witness is, do you think there needs to be any updating to the Act in relation to recognition of economic impacts, looking at the impact that very real recommendations can have if they are parroted by political Parties that recommendations can have on real investment dollars and real community development, and if there is language in this Act that should be updated to reflect our mandate as a government to protect those matters of public interest?

CATHERINE TULLY: In terms of the exemptions that are in the Freedom of Information and Protection of Privacy Act, including the economic exemptions, those are very standard in laws across Canada, and they've been around for quite a long time. They seem to have worked quite well in all jurisdictions in terms of setting a reasonable standard, balancing the economic interests versus the very important accountability interests and foundation of the Act.

In the recommendations that I made, I didn't recommend changing too many of the exemptions because, as I said, they're standard and fairly tried and true, but this is something that would be part of a discussion about updating a law, is examining how well it has worked, and whether it represents the interests and the balance that Nova Scotians believe should be represented.

ZACH CHURCHILL: I thank you for allowing me to get to my question, Mr. Chair. That's appreciated. I'll pass further questioning to my colleague.

THE CHAIR: Mr. MacKay.

HUGH MACKAY: Thank you, Ms. Tully, for being here. We certainly hold the workings of the Office of the Information and Privacy Commissioner - as well as that of the Office of the Auditor General and that of the Ombudsman - in a great deal of respect and with our gratitude for the services that you provide in helping us improve government and delivery of services and open and transparency in our dealings to the public.

My colleague just mentioned perhaps one certain condition or one aspect of the privacy Act that perhaps could be revisited in regard to economic interests. I think government is constantly looking at what we have to do to change various Acts. The Residential Tenancies Act, for example, with the onset of the wave of the sharing economy that has come in and how that impacts on tenancy Acts - there are always things with traffic Acts, fisheries Acts, and so forth, that require modernization.

I'm bringing this up in regard to the comments previously in regard to the action plan that the department has created. We sort of slipped from the action plan perhaps over to modernization of the privacy Act. I'd like to return to the action plan itself. First, the action plan, I'm sure you've reviewed it, is publicly available for all.

There are a lot of projects under way, activities under way, to address the recommendations in that. The department has hired Deloitte to conduct a post-event, lessons-learned type of review, and I believe that's going to be released shortly. I'm wondering, what are your thoughts on integrating the actions of your office with that of the Office of the Auditor General and the Deloitte reports - of integrating these?

CATHERINE TULLY: If I understand you correctly, it completely makes sense to me that there may be one action taken that addresses a variety of recommendations. Of course, I think they want to be efficient; they want to do things that are effective. They don't want to just spin their wheels, so I am very interested in seeing actions that may have multiple effects, that address a variety of issues, and that make complete sense to me. I wouldn't be surprised at all if they didn't choose a strategy that addresses a bunch of recommendations. Is that kind of clear?

HUGH MACKAY: That addresses my question, thank you. In my review of the action plan, it would appear to be - to my view, again - that the department has a response to each of the recommendations that you've made and that they have agreed to co-operate with your office. I think you mentioned previously that you will be meeting with them. Can you elaborate on meeting with them? Is this going to be done on a regular basis? Have you any indications from them how that will move forward?

CATHERINE TULLY: The minister indicated an interest in ensuring that we meet quarterly - that in addition to dealing with these recommendations that they will provide us with an update on new projects and ongoing projects, and they will provide us with privacy impact assessments if we ask for them - kind of a new relationship with our office, which I think is an important step forward. I certainly appreciate it.

HUGH MACKAY: Would you agree, then, that it's fair to say that the department is responding in a proactive manner regardless of looking in the rear-view mirror? Are we now moving forward in a very proactive manner to ensure that there are greater securities in place for protection of information?

CATHERINE TULLY: I think we're definitely moving in the right direction. Absolutely, yes.

HUGH MACKAY: I'll pass to my colleague.

THE CHAIR: Mr. Jessome.

BEN JESSOME: Ms. Tully, thanks for being here. I wanted to talk a little bit about or get your perspective on your relationship with the Office of the Auditor General throughout this process and how the coupled or two-pronged approach to reviewing this circumstance lent itself to coming to the conclusions that needed to be put there and that we as a government intend to respond to.

CATHERINE TULLY: We each engaged in our separate processes. What we did decide though was, where it made sense, to interview witnesses together to keep them from having to answer maybe even exactly the same questions twice. It made sense for us to interview together. We had different tests, we had different standards, and we had different approaches, but we could gather evidence together. Where it made sense, we attended the same interviews and asked our questions and went away. We wrote our reports separately and didn't actually share recommendations or anything until they had already been shared with the department. It's interesting that we reached basically the same conclusions. That's good, because we heard the same evidence.

From my perspective, it was a very useful approach. My office doesn't have the kind of security expertise we needed to truly understand the cause of this, so it really helped us to have the Auditor General's expertise. We did our own research as well, but it helped to have their expertise in terms of designing some of the security questions. That's the one place where we sought some input from them. Overall, I believe the product of the two reports contributed quite a bit to moving forward in terms of how we do better.

BEN JESSOME: Hearing that positive feedback about the relationship between the two offices and the ability to respond to this breach and to be critical of the protocol that was not in place in this case from this breach, is it a fair statement to say that there is reasonable oversight in place presently with respect to the capacity of the two bodies, the Office of the Auditor General and the Office of the Information and Privacy Commissioner?

CATHERINE TULLY: So my office is what you're referring to?

BEN JESSOME: Yes.

CATHERINE TULLY: It worked well in this case, but I have pointed out some of the shortcomings. We investigated because they notified us of this breach. They don't have to. Breaches can be happening that we wouldn't know about. There's no obligation. There are some important improvements, so I wouldn't say that it's adequate yet. We certainly do our best. I think that it worked well in this case.

THE CHAIR: Order, please. That concludes time for questioning. Thank you, Ms. Tully, for your insight and your answers to questions that are important to the Province of Nova Scotia and the public. If you wish, there's a little bit of time to wrap up.

CATHERINE TULLY: Thank you all for your questions today. I appreciate the interest in the work of my office. I also always enjoy hard questions, so I appreciate that too.

Thank you to the people in the Department of Internal Services. I appreciate how challenging this investigation was for them. I also wanted to thank the Auditor General and his staff. We engaged in a collegial process that led, I think, to very significant reports on this issue.

Finally, I want to thank the people in my office. I have the benefit of the support of a group of very clever access and privacy experts. It's an honour to lead this small but dedicated group of professionals.

THE CHAIR: Thank you very much. We will take a two-minute recess to allow Ms. Tully to vacate the premises, I guess, for lack of a better term, and we have committee business to take care of.

[10:45 a.m. The committee recessed.]

[10:46 a.m. The committee reconvened.]

THE CHAIR: Order, please. We'll reconvene the committee. We do have some correspondence from the Department of Internal Services on information requested at the February 20, 2019 meeting. I think everybody has that information in front of them. Are there any questions or comments on the information? Thank you very much.

The next item on the agenda is the Auditor General reporting dates. As the committee will now be meeting only once a month, we have to figure out how we're going to deal with the following issues related to the Auditor General's Reports. On previous months when the Auditor General was reporting, what will the procedure be? Previously the committee would meet with the AG the day after the report was tabled and then the committee had previously agreed to the practice of meeting with the AG and the Deputy Minister of Finance and Treasury Board when the annual financial audit is presented. What are the procedures going to be? Mr. Wilson.

GORDON WILSON: Thank you. I appreciate the clerk wanting clarification on these. I understand our March 12th meeting is filled. We have a witness coming for that. I believe at the end of March we have the AG's Report coming out, Mr. Atherton, I think, if that's correct.

What I would simply suggest is that the April 12th meeting would be the meeting date that we would have with the AG. I know it would be nice in future dates if - there has been some discussion back and forth with the committee on how we meet with the AG to go over these. We did some adjusting. There were some comments on even having a longer

time frame between the report coming out and meeting with the AG. I'm sorry, it's the 13th.

What I would suggest is that if it's possible for the AG, now knowing when our times are, if he would like to release future reports at another date just prior to the timing of the Public Accounts Committee, that would work well. If not, simply we would just fall in line, have the AG come in at our next date that we would have immediately after his report that would come forward. Then subsequent to that, the next dates after that of our committee meeting would simply be filled with the chapters, all the chapters that we've agreed to review and the witnesses.

I know that we've talked to the clerk about flexibility and not having Chapter 1, Chapter 2, Chapter 3, so that we would just continue on with that process. We also have a follow-up report coming out from the AG. I would assume that the proper, easy way to do it would be to simply have that follow-up report scheduled into the first available meeting that we would have.

Also, I do agree that when the financial report comes out, I think we should still continue with the practice of having that scheduled again at the first available Wednesday that would be available. We know when these reports are coming out from the AG, or roughly when, so it's not a real stretch to be able to do that easily and have the deputy minister at that same meeting when the AG's Report is tabled. I think that is a practice that we recognize was used in other jurisdictions and we'd like to follow.

THE CHAIR: Ms. Leblanc.

SUSAN LEBLANC: I was going to go at this in a different direction, surprisingly. Given the Auditor General's packed schedule and all the work that the office is doing, I think it's rather unfair and somewhat insulting to ask the Auditor General to all of a sudden accommodate the new schedule of the Public Accounts Committee.

What I was going to suggest is that if there is an Auditor General's Report that comes out and there is not a PAC meeting - for instance, it comes out on a Tuesday or whatever and it's not a week that a PAC meeting is scheduled, then we add a meeting for that particular week so that we can continue to hear the Auditor General's Reports as soon as possible and discuss them with him. Then the regularly-scheduled PAC meetings, which are the second Wednesday of every month, would be in place to hear the witnesses connected with those.

If there was an Auditor General's Report that happened to be - like the scheduled day was in accordance with the second week of the month, then sure, let's talk about it at that PAC meeting, but if it's not, then let's add a meeting so that we can make sure we hear them promptly without asking the Auditor General and the office to adjust their plans.

THE CHAIR: Ms. Roberts.

LISA ROBERTS: I would absolutely like to see us move forward on that basis. In fact, there has not ever been a conversation at this committee about allowing some time to lapse before we heard from the Auditor General's Office related to specific reports. We have talked about perhaps allowing some time to lapse before we hear from the departments as part of our follow-up, but there was never a conversation about not hearing from the Auditor General on the day following the tabling of each report.

If we do not add a date to accommodate the Auditor General's schedule, my concern is that we are then virtually giving up on what had been a committee effort to commit to better follow-up, because we will then be using our monthly meeting to hear from the Auditor General related to reports.

What happens when the Spring report comes down, which will be dealing with not just one department but several departments? We don't know what is going to happen with the March 27th report, which is the two-year follow-up. We don't know which of the departments or which of the previous audits will show that there have been issues with follow-up. How are we to schedule those relevant departments for follow-up, as we have committed as a committee, as is our mandate, if we don't have the dates available in our calendar under this new regime?

So please, let's add dates to accommodate Auditor General topics, and then we'll try to get the departments in on the other meetings on a monthly basis.

THE CHAIR: Mr. Halman.

TIM HALMAN: I have been clear that this whole process - I'm against these changes. If what they're proposing can minimize the damage, we'll go with it. I get that.

I'm curious as to what the clerk may think as to this being put out there. At the end of the day, this will have to be facilitated by your team. What are your thoughts?

THE CHAIR: Ms. Langille.

KIM LANGILLE: To which option? To both? Really, it's up to the committee. I can make either work.

THE CHAIR: Mr. Wilson.

GORDON WILSON: I appreciate the comments and I understand the pushback from the members on this, but respectfully, we have decided to go with the monthly meetings. I see no reason why a logical transformation of bringing forward . . .

THE CHAIR: You have decided? The committee has to decide.

GORDON WILSON: Can I finish, Mr. Chair? I feel that this is an easy, logical move.

I'd also like to add the point that let's not lose the fact that the request to have all of the Auditor General Reports come before this committee was the request of the Auditor General. Prior to that, we were only meeting 20 per cent of those chapters that were coming here. This is 100 per cent.

I would like to make a motion that the meeting dates of the second Wednesday of the month be the dates that the Auditor General's Reports come forward and that the subsequent dates of any reports from the Auditor General be brought forward as soon as possible on those second Wednesdays of the month.

SUSAN LEBLANC: Can we have a little recess for two minutes?

THE CHAIR: If we recess, we'll have to extend the time. Is everybody okay with that? Granted.

[10:55 a.m. The committee recessed.]

[11:00 a.m. The committee reconvened.]

THE CHAIR: Ms. Leblanc.

SUSAN LEBLANC: I would like to make an amendment to the motion. Our amendment would be . . .

GORDON WILSON: You can't make an amendment to a motion. If there's a motion on the floor, it has to be dealt with . . . (Interruptions)

THE CHAIR: Why can't you? You have to deal with the amendment first before you can deal with the motion, if there's an amendment made.

Ms. Leblanc.

SUSAN LEBLANC: Our amendment would be that the Public Accounts Committee would hear Auditor General Reports on the Wednesday following the release of the report if that Wednesday is not already a scheduled Public Accounts meeting. We further move that additional meetings will be scheduled throughout the year as required in order to ensure follow-up with departments connected to the Auditor General Reports.

THE CHAIR: Comments on the amendment? Mr. Halman.

TIM HALMAN: Regardless, what we're talking about here is government being less transparent. Either way, the whole thing stinks. What we want is to see more transparency. This conversation, to me, is the worst place for us to be in. We're now at this point where this committee cannot meet once a week. This committee cannot question government spending weekly. We're talking about less transparency in government.

Look, I don't want to be a part of this. This is not right. This isn't right for Nova Scotia. I have been clear about that. We need more transparency in government. We can put this motion forward and add this amendment, but either way, that's what we're talking about - less transparency in government. That's not right.

LISA ROBERTS: I would just like to remind the committee - and some members of the committee would not have been sitting at that time - that in September 2017, the Auditor General raised concerns about Auditor General Reports not being followed up on by this committee

I think it's relevant, and my former colleague David Wilson shared with me his perspective, which is that in the previous year there had been an election, so there had been an interruption of the work of the committee for the provincial election campaign, and then the committee was not reconstituted until September. There was about a four-month period in the year immediately previous to the Auditor General making that comment to us, when the committee did not meet as often as it normally does, which contributed to it getting behind on doing follow-up meetings.

Also, while it is important that the Public Accounts Committee works and operates in a non-partisan fashion looking at government administration and how the government spends taxpayer dollars, it is widely recognized that it is more difficult to maintain that non-partisan tone as you approach an election, which was indeed the case in May 2017.

I think it is very important now, when we are still several years out from the next provincial election, that we recommit ourselves to working in a non-partisan fashion and in collaboration with the Auditor General, which would involve scheduling adequate times to at least hear from the Auditor General when reports are tabled and do follow-up on those recommendations.

THE CHAIR: Ms. Leblanc.

SUSAN LEBLANC: Look, we wouldn't be in this position to be constantly discussing this issue over and over again had the change not been made in the first place to limit the number of times Public Accounts meets.

The fact is that we know that we do not have enough time in 12 meetings a year to hear the Auditor General Reports and do the proper follow-up to call the right witnesses to actually get to the heart of those reports and hold the government to account and figure out

the way the money in this province is spent. There's simply not enough time. I can't do the math that quickly, but we would be going into years, much further than we are right now, if we were to go on the current schedule.

The fact is that we need more time. This amendment to my colleague's motion is a reasonable suggestion around this particular conundrum that comes with these changes that the Liberals have made to this committee.

I reiterate, all we would be doing is adding a meeting. When the Auditor General releases a report on a Tuesday, we add a meeting on the Wednesday to hear his comments as the committee. The rest of the regular-scheduled meetings are then filled up with the witnesses that come from those reports. It seems like a no-brainer.

I think the people of Nova Scotia, I'm hearing, are angry at these changes and this would be a way to mitigate some of the problems that have happened since these changes have been made - or will happen. I strongly encourage people to vote for my amendment. Thank you.

THE CHAIR: If there are no further comments, would you please read the amendment again, Ms. Leblanc, and we can vote on it.

SUSAN LEBLANC: The amendment is that the Public Accounts Committee would hear the Auditor General's Reports on the Wednesday following the release of a report if that Wednesday is not already a regularly-scheduled Public Accounts Committee meeting. We further move that additional meetings will be scheduled as required, in order to ensure proper follow-up with departments connected to the Auditor General's Reports.

THE CHAIR: Would all those in favour of the motion please say Aye - there has been a call for a recorded vote.

YEAS	**NAYS**
Tim Halman	Hugh MacKay
Lisa Roberts	Zach Churchill
Susan Leblanc	Ben Jessome
Eddie Orrell	Suzanne Lohnes-Croft
	Gordon Wilson

THE CHAIR: The motion is defeated. Back to the main motion. Mr. Wilson.

GORDON WILSON: I understand that the motion that I've put forward you'd like that in writing? Or should I just reword it, re-say it again, Mr. Chairman?

THE CHAIR: Just reword it.

GORDON WILSON: In a simpler term, I just simply move that the AG Reports come to the Public Accounts Committee on the first available scheduled date available, and that subsequent chapters of the AG Reports be scheduled at regularly-scheduled Public Accounts Committee meetings as they become available.

Just a couple of comments I'd like to make on that. The statement that this would not be able to bring all the Auditor General's Reports is simply not quite accurate. We have two reports of the AG, a Spring and a Fall, with three chapters, usually with each one of those. That's eight meetings.

We usually have a follow-up meeting from the AG once a year also. Now we're at nine. The AG does, on occasion - he has a financial report that comes out. We're now at 10 meetings. We do have on occasion a couple of other audits that the AG does, so if we look at 12 meetings a year, I do feel very comfortable that we're going to be able to bring not only all of the Auditor General's Reports, but all of the subsequent chapters that follow that, to bear here at the Public Accounts Committee in a timely manner.

As far as the comments around the partisanship, who is more non-partisan than the Auditor General to serve Public Accounts? Who is the person who is entrusted with the responsibility of being objective and thorough in bringing the concerns forward? I think that's an important part for us to understand that we have that.

On the topic of transparency, I'd like to note just a few things. We as a government have done a lot of good things, I believe, that are being missed, and this transparency issue keeps being brought forward. We've created an open data portal for hundreds of sets of information to be able to be seen by the general public. We have our Crown land harvest maps that are now available for the general public to see. Our Fisheries and Aquaculture mapping tools have a very transparent layer there for all of the general public. Our waiting times for our residential nursing homes and long-term care facilities are available.

Our senior officials' expenses are now posted online for all of our senior officials. These are all new things, Mr. Chair. FOIPOP applications - we've seen the largest amount of FOIPOP applications of any government, and we've increased our response to 80 per cent within 30 days, so we are being extremely transparent.

We have a Health Committee now that we've created that's being televised and we have a Premier who attends chambers of commerce meetings without a script, sits down, and answers every question that is asked of him.

When people challenge us about transparency, I think there's a real story to be told there. I'd just like to add those comments. I'd like to see our motion go forward, and as the clerk had noted, it's not a difficult thing for her to schedule all that stuff in there in that order. I'll leave it at that.

THE CHAIR: I'd like to ask Mr. Atherton if he could comment on the ability for the Auditor General to do that reporting around our schedule instead of his own.

ANDREW ATHERTON: I think first, I would need to clarify. I'm not clear whether the motion expects that we will report in conjunction with your meetings or if we will simply be called when you have meetings and we'll report when we're able.

GORDON WILSON: I think it would be nice if you could work your schedule around reporting as you did prior to our meetings, but certainly it's your privy to bring the reports forward at your wish, and then the first available meeting of the Public Accounts Committee is when we hold our open meeting with that.

ANDREW ATHERTON: We will do what we can to accommodate the schedule of the committee. I know for our next three reports for follow-up - I guess a month from yesterday, March 26th, for ALC follow-up, which is coming out April 16th, and then our Spring report is May 28th. None of those are able to be moved and unfortunately don't coincide with your meetings.

LISA ROBERTS: Can I ask Mr. Atherton to clarify how many substantive audits does the Auditor General's Office produce in a year typically?

ANDREW ATHERTON: Typically, we would have follow-up. We usually have two performance audit chapters, which would be three to four chapters each. We have our financial report in the Fall. We've often in recent years had additional work such as what was discussed today - the privacy chapter.

So probably the average is nine or 10. If we consider our follow-up work as a single entity, when in reality it covers all the entities we've looked at in the last two years, so another dozen to 15.

LISA ROBERTS: When you talk about those performance audits, I believe in the past we would have looked to call each of those chapters separately because each of those chapters is dealing with different substance and often different departments.

ANDREW ATHERTON: One performance audit report would have three to four chapters, which yes, would cover different entities.

LISA ROBERTS: My math is getting to 10 to 12 only dealing with the substance of your office's work without ever leaving a blank date in which to call a government department. We seem to be challenged with the math of even the most basics of 12.

THE CHAIR: Any further comments?

A recorded vote has been called for. Would all those in favour of the motion, please say Aye. Contrary minded, Nay.

YEAS	**NAYS**
Mr. MacKay	Mr. Halman
Mr. Churchill	Ms. Roberts
Mr. Jessome	Ms. Leblanc
Ms. Lohnes-Croft	
Mr. Wilson	

THE CHAIR: As Chair, I vote no.

The motion is carried.

There is no further business. The committee is concluded. The next meeting will be March 13th, 8:30 a.m. to 9:00 a.m. an in camera with the AG for a briefing and 9:00 a.m. to 11:00 a.m. with the Department of Internal Services.

The meeting is adjourned.

[The committee adjourned at 11:14 a.m.]