M-17

ISSN 1180-436X

Legislative Assembly of Ontario

First Session, 41st Parliament

Official Report of Debates (Hansard)

Wednesday 21 October 2015

Standing Committee on the Legislative Assembly

Petitions

Chair: Monte McNaughton
Clerk: Trevor Day

Assemblée législative de l'Ontario

Première session, 41e législature

Journal des débats (Hansard)

Mercredi 21 octobre 2015

Comité permanent de l'Assemblée législative

Pétitions

Président : Monte McNaughton
Greffier : Trevor Day

Hansard on the Internet

Hansard and other documents of the Legislative Assembly can be on your personal computer within hours after each sitting. The address is:

Le Journal des débats sur Internet

L'adresse pour faire paraître sur votre ordinateur personnel le Journal et d'autres documents de l'Assemblée législative en quelques heures seulement après la séance est :

http://www.ontla.on.ca/

Index inquiries

Reference to a cumulative index of previous issues may be obtained by calling the Hansard Reporting Service indexing staff at 416-325-7410 or 416-325-3708.

Renseignements sur l'index

Adressez vos questions portant sur des numéros précédents du Journal des débats au personnel de l'index, qui vous fourniront des références aux pages dans l'index cumulatif, en composant le 416-325-7410 ou le 416-325-3708.

Hansard Reporting and Interpretation Services
Room 500, West Wing, Legislative Building
111 Wellesley Street West, Queen's Park
Toronto ON M7A 1A2
Telephone 416-325-7400; fax 416-325-7430
Published by the Legislative Assembly of Ontario

Service du Journal des débats et d'interprétation
Salle 500, aile ouest, Édifice du Parlement
111, rue Wellesley ouest, Queen's Park
Toronto ON M7A 1A2
Téléphone, 416-325-7400; télécopieur, 416-325-7430
Publié par l'Assemblée législative de l'Ontario

LEGISLATIVE ASSEMBLY OF ONTARIO

ASSEMBLÉE LÉGISLATIVE DE L'ONTARIO

STANDING COMMITTEE ON THE LEGISLATIVE ASSEMBLY

COMITÉ PERMANENT DE L'ASSEMBLÉE LÉGISLATIVE

Wednesday 21 October 2015

Mercredi 21 octobre 2015

The committee met at 1304 in committee room 1.

PETITIONS

The Chair (Mr. Monte McNaughton): Good afternoon, everyone. Welcome to the Standing Committee on the Legislative Assembly. A gentle reminder that our meetings start at 1 o'clock on Wednesdays. We are—

Interjections.

The Chair (Mr. Monte McNaughton): It's true. We are a few minutes late.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

The Chair (Mr. Monte McNaughton): I'd like to welcome our first presenter, Brian Beamish, the commissioner of the Office of the Information and Privacy Commissioner of Ontario. Brian is going to have 30 minutes for presentations, and we'll divvy up the time that's remaining for questions from each party.

Mr. Brian Beamish: Good afternoon, everybody. I am Brian Beamish. I'm the Information and Privacy Commissioner for the province. Thank you very much for the invitation to come and participate in your deliberations and discussions around e-petitions. I'm very appreciative of the opportunity.

We have prepared a written submission that we've handed out, but I thought maybe in my comments I would give you an overview and summary of what's in there.

Just as a preface, my office, as you know, is an independent office. We provide an independent overview of government decisions around access to information and privacy. We also have a consultative role, and it's in that role that I'm speaking to you today.

As the title suggests, though, I do wear two hats. I am the information commissioner, where we focus not only on the formal access to a freedom-of-information regime but also larger issues around open government, transparency and accountability. And I'm the privacy commissioner, where we focus in on the privacy rights of the citizens of Ontario. I'll be making comments to you today wearing both of those hats.

First of all, let me start by recognizing the importance of the petition process even as constructed today in paper form. In my view, public petitions allow the public an opportunity to interact with their government and have a voice in what government is thinking and doing. It helps to engage citizens in the activities of government and contribute to responsive government.

I know that you have, in your deliberations, looked at examples of other jurisdictions that have gone the extra route, from a paper petition process to the e-petition process. I think that's a very valuable step and certainly one that our office supports as moving the petition process into the realities of today.

Let me put my information commissioner's hat on and focus on the positives of e-petitions as they contribute to openness of government.

As I said, the primary activities of my office in terms of access or open government is on the formal freedom-of-information regime. People put in a request for information and, if they don't like the response they get from government, they come to my office. But we really see that formal FOI regime as a small part of a larger effort to open up government, provide citizens with access to information that government is holding, and achieve transparency and accountability through that.

In this regard, an e-petition, in our view, would contribute to public engagement—provide the opportunity for greater public engagement. That's makes it a positive thing. We certainly view an e-petition process as contributing to Ontario's open government efforts. You will know that jurisdictions around the world are moving to a more open government process. As I understand, and as I've tried out the current petition system, an individual really doesn't have a way to find out what petitions might be under way unless they're approached by someone who has a paper petition or, in my case, somebody might approach me at the curling club or what have you. Individuals won't find out what petitions have actually been presented and what responses are from the government unless they check Hansard, which can be a very laborious effort, and dig through that. It puts individuals to a lot of effort to find out what's going on in terms of petitions.

E-petitions I think can address that. People will be able to find out what petitions are under way and make a decision on whether they want to participate in that process. They will also have an opportunity, if that is part of the process that the government needs to respond, to see what the government response is, and that can be

done without having to plow through Hansard or go down to the Clerks' office to find out what petitions have been presented.

In my view, it's going to foster greater participation, but at a minimum it seems to me that it's going to make the process more convenient and more accessible. It will allow citizens to engage with their government in the manner that they're becoming accustomed to, and that is electronically. People are increasingly not wanting to engage in government in a paper process.

1310

Two weeks ago, I was able to renew my licence tag online. It took me 90 seconds. That's the way I want to engage; I don't want to have to go down to the bureau and stand in line for half an hour. That kind of thinking applies to the e-petition process. At a minimum, people are now going to be able to have a more accessible and a more convenient process.

Let me just say a few words about the design. I know you've spent a lot of your deliberations around how this process might be designed. There are, I think, some key questions around the criteria for filing an online petition: What information would be collected from the creator and the signatories of a petition? How do you verify signatures? Is there a threshold for petitions going active and another threshold for petitions requiring a response from the government?

These questions all have some significant impacts in terms of privacy that I will get to, but I think that how the system is designed will also impact its accessibility and usefulness for the public. For example—the examples we've looked at and that you've looked at—there would be a threshold for a petition being active, available for individuals to support, and, in some cases, a second threshold where some kind of government action would be required. That might be simply providing a response; it might be the possibility of a debate in Parliament. In any event, there is a second threshold that would require some positive action. It would seem to me that to encourage citizen participation, that primary threshold, in terms of when it would go active, should be relatively modest. We would support a second threshold that would say, "If you gather a certain number of signatures, then the government is obliged to do something." That may be as simple as a non-binding response, but at least it might provide some meaning to the process for the people who do support a petition.

One of the other issues that I know you've grappled with is: How do you verify the legitimacy of the signatories who are signing? How do you ensure that you have one individual, a real individual, and not somebody who has hacked into the system, who is using an automated program to generate a lot of signatures? You'll see that in our paper we've offered some solutions to that. The one that seems most apparent, the one that you've heard of, is to employ the CAPTCHA method to go a long way towards eliminating the ability of an individual to use an automated program to generate a large number of signatures.

Finally, before I leave this issue of design, it may sound simple, but I think that some thought should be given to things that might seem as mundane as the length of the petition. In my view, you would want to permit a length that is enough to allow people to state their case and say what it is they want government to do. However, I think there can be a danger in making it too long. I've seen some of the petitions on other sites, and I get lost in the "whereases." To me, the shorter, the better, and the quicker the people come to the point, the better. The quicker people come to the point, the more accessible it is for the public in general. I would ask you to give some thought in terms of the length.

Let me turn to the privacy implications of this because my guess is, that's the primary reason why I'm here. I'm really happy, first of all, to see that in your discussion so far, everybody I've seen recognizes that this is going to involve the collection of personal information of the citizens in Ontario, and that that raises issues that need to be grappled with in terms of privacy. I was also pleased to recognize that, although the Legislative Assembly itself is not covered by our formal privacy laws, I think everyone is in agreement that, although, not technically or legally required to put in privacy protections, that's the thing to do. That has to be done. This program cannot be introduced in a way that intrudes inappropriately on the privacy of the citizens of Ontario. I think those are two very good starting points in terms of implementing the program.

We're looking at a system here where, presumably, someone creates the petition, puts it out on offer for people to support, and individuals will make a decision on whether they're going to support that petition or not. The decision to support a petition is going to involve, at some point, the provision of their personal information, just by the design of the program. I think it's important to think about the nature of that information they may be providing and some of the qualities about that. I look at three ways to describe that information: It's potentially very sensitive, it's attractive and it's digital. I think those three qualities will drive some of the protections that are put in place.

I say "sensitive" because not only are individuals presumably providing some information to identify themselves in contact information—it may be a name, it may be an email, it may be their address—but the fact that an individual supports a particular petition may very well tell you about them, and something that's very sensitive about them. It may talk about their political beliefs, religious beliefs, social beliefs, likes and dislikes, and that can be very sensitive information. Protections need to be put in place to recognize that.

I say that it's attractive because I think we can all understand how a list of individuals who support a particular cause plus their email address would be very attractive to political parties, non-governmental organizations, interest groups, commercial enterprises. In many ways, it can act as an easily made list of supporters or potential clients or customers. It potentially is a very

attractive list and therefore there need to be some protections put in place around it, and I will speak to that.

The third quality that I mentioned was that it's digital. We would no longer be in the paper-based world, where what we call practical obscurity protects the information. You would have a list of individuals, the cause they support and contact information for them available in digital form, which would be very useful, very usable, very easy to manipulate—much more than having to go down to the Clerks' office and dig out a paper petition. So those three qualities make the information that's being collected very attractive and very susceptible to profiling individuals and very susceptible for use in terms of delivering political or commercial or other messages. That, to me, sets out the need for a framework around how this information is going to be managed. So let me turn to that.

The first question I look at is what personal information should be collected to start with. To answer that question, I start with the idea that one of the basic tenets of privacy is what we call data minimization. That says that you only collect the information you need to fulfill the purpose that you have at hand. You don't over-collect information. In terms of an e-petition and, say, someone who is supporting an e-petition, you might want to verify their residency somehow, that they're a resident of Ontario, that you have an individual and some way to measure that this is a unique individual and not someone who is signing this petition 100 or 1,000 times.

But keep in mind that the information collected has to be proportionate to what the purpose of the program is here. This e-petition process I would contrast to, say, the referendum to—a recall referendum. Sorry; I got stuck. If you have a process in place where a certain number of signatures can be collected and that will automatically require a vote on whether a member is recalled, that has significant impact. We're not talking about that here. We're talking about potentially at most a non-binding government response. So I think that tempers the type of information that may be required here, and as we review the various systems that are in place or the programs in place, we feel that collecting a name, an email address and a postal code would be sufficient to verify that you have a resident of Ontario and that you've got a real person. We feel that's proportionate to what the goal of this program is.

1320

There may be different considerations in terms of the creator of the petition. That individual is asking other people to support their idea and their concept. I think in that case, it may be fair that their identity be known to people so they know who it is that is putting that request out for their support. I know that in some of the examples that you've seen and that I've seen, the name of the creator is available—not their contact information, but at least, then, people going in and making a decision about whether to support the petition or not know who it is that's originated it.

I think a really important second question is: Who should have access to that information once it's collected? So let's say you've collected the name and email address and postal code, or full address, of signatories; who should have access to it? I mentioned how this is potentially a very attractive source of information for a wide variety of groups, but it's being collected solely for the purpose of instituting an e-petition process. Because of that, in my view, there should be tight restrictions placed on it so that only those staff who are implementing the e-petition process have access to this information.

I guess I've made an assumption that this would be operated by the Legislative Assembly itself, so I would say that only the administrative or technical staff of the Legislative Assembly responsible for implementing the program should have access to it and it should be strictly off-limits for any other groups, whether that's a political party, third parties, commercial enterprises, special interests groups, what have you. I think this is a key issue that will need to be addressed in order for the e-petition process to be successful.

A third question we looked at was: Having collected the information and put some restrictions on who has access to it, what is it that goes up on the e-petition website?

Again, here is where we get into a world that is different from paper petitions. I understand that an individual could go down to the Clerks' office and have a paper petition pulled, which will have attached to it the people who support it and their name and address, but this is a much different process and we would highly recommend that the only thing that appeared on the website was the petition itself and the number of people supporting it, and that the identity of the people who have supported—the signatories—not appear. I think that's pretty consistent with examples of e-petition processes out there, that the names and the identities of the people who have supported the petition, who have signed on to the petition, are not made public.

Now, again, there may be a different consideration when it comes to the creator of the petition itself. I know that in some examples we've looked at, the creator's name would appear on the website. I think there are good arguments for that as well, but again, I would limit the amount of information about the creator that would appear, certainly not their contact information.

If I can move on to say a few words about safeguards that should be put in place—because the safeguards that are put on this information are really important to preserve the privacy of the individuals who are participating in the program. Privacy is not all about security, but you can't have privacy unless you do have security.

The fact that there will be a database of personal information about individuals requires that measures be put in place to ensure that that information is secure, that it's not being used for improper purposes, that it's safe from unauthorized access, and that it's safe from being hacked into, that there are security measures in place.

You'll see from our paper that we distributed, we're recommending things like encryption, when the informa-

tion is in transit or at rest; clear controls on access to the information; some type of audit logs on who is looking at the information, to ensure that those people who are going in and looking have authority to do it, and that there is a way to check that; and also training—that staff of the Legislative Assembly who are involved in operationalizing the program are well trained in terms of their responsibilities.

I draw some experience here from work that we've done in the hospital sector. Hospitals clearly have a lot of very sensitive personal information. They have the same issue: How do you ensure that that information is safe from intrusion and kept secure? We have spent a lot of time dealing with things like unauthorized access, where people who don't have the right to see that information have gone in and looked at it. So there are lessons to be learned out there in other sectors that have grappled with this issue.

We have looked at another issue around the retention of the personal information: Once it's collected and an individual has signed up, has become a signatory, how long should their information be collected? Again, one of the basic principles of privacy is that you only keep information as long as you need it. Once it's no longer needed, the longer you keep it around, the greater the chance that something bad will happen.

I would encourage you to take a look at that issue and make a determination on how long this information is useful. It would seem to me that it may be useful as long as a petition is open for signature, but once it's closed I question whether that information is necessary to be retained. There may be archival reasons for keeping that information. I'm not an expert in that area, but if it's thought that there is a need to keep signatory information longer than the life of the petition itself, then perhaps there are ways to look at how to reduce the risk of that; for example, not keeping the information in digital format but keeping it in a hard-copy form.

I want to close out by making a couple of final points. One is that whenever an institution is implementing a new program like this, we really encourage them as a best practice to have a very clear and concise privacy policy. I've looked at some of the other examples out there and there's a real mixture in terms of policies that are available. Some are very good in terms of describing to the public what the program is about, what information they will be collecting, and how that information will be used. I think it's really important that people be able to find out very quickly and very easily from the website what the expectation is if they do create a petition or if they sign a petition. It should be very explicit to them what will and will not be made public and how that information will be used. I really encourage the Legislature, if it goes this route, to have a really clear, simple-language, easy-to-find privacy policy that delineates all of these issues. Let people make an informed decision on whether they want to participate.

My final point I wanted to make is that there are a lot of issues to think about, a lot of questions to ask, but luckily there is a way—I think a good method out there—to ensure that these questions are asked and addressed before you go live and flip the switch on an e-petition program and that is something called a privacy impact assessment. This is a well-recognized risk management tool both within government and in the private sector—a very common best practice when a new program is being introduced, to undergo a privacy impact assessment. It's a way that you can ensure that the right questions have been asked and the right answers are in place, that they're done at the beginning of the program, so that you're not trying to play catch-up when you find problems along the way.

We're lucky in Ontario. The Ontario government, particularly the Ministry of Government and Consumer Services, has an excellent PIA tool. They have very knowledgeable and skilled staff. I think, should the Legislature decide to do a PIA, you would find that they would be really helpful. I can also say, I can offer the services of my offices, to the extent that we can be a resource in undergoing that process before the e-petition process goes live.

Those are my comments. I want to thank you again for the opportunity to speak. I think this is a really good program that can be put in place while respecting the privacy of the citizens who are engaged in it.

The Chair (Mr. Monte McNaughton): Excellent.

Mr. Brian Beamish: Thank you.

1330

The Chair (Mr. Monte McNaughton): Thank you very much, Mr. Beamish. We'll allow 10 minutes of questioning from each party. We'll begin with the official opposition. Mr. Clark.

Mr. Steve Clark: Thanks, Mr. Beamish, for coming today. I appreciated receiving your submission and your comments.

Mr. Beamish, the government's been reviewing e-petitions now for some time and I just wondered if, over the last few months, they had ever engaged you prior to coming to today's meeting to give them suggestions on e-petitions policy.

Mr. Brian Beamish: This is the first time I've been consulted about e-petitions. I was aware of the issue coming up with the government engagement report that was released prior to the last election. I'm happy to see that they recommended e-petitions, but it's the first time I've been consulted on it.

Mr. Steve Clark: The reason I'm asking is, we've been talking about this since February, so I am a bit disappointed that the government hasn't reached out to you before that because I know they've been having their own internal discussions about this.

Ms. Eleanor McMahon: He's here now.

Mr. Chris Ballard: It's the job of this committee—

The Chair (Mr. Monte McNaughton): Order.

Mr. Steve Clark: So I can't have 10 minutes for questions?

The Chair (Mr. Monte McNaughton): Yes, go ahead, Mr. Clark.

Mr. Steve Clark: Thanks, Chair. Right now, the—

Interjection.

Mr. Steve Clark: Are you done, Mr. Ballard. Are you done?

The Chair (Mr. Monte McNaughton): Order.

Mr. Clark.

Mr. Steve Clark: There are a number of members from all three parties that use e-petitions on their websites presently. I see the privacy policy suggestions here starting on page 6 and on page 7, and I guess one of the things that I'd like to suggest is that you send out to all 107 MPPs—106, I guess—those comments about e-petitions.

I know with my own e-petitions—I've had a couple of them and I know the expectation that people have when they sign the e-petition. Many of them expect that I'm going to communicate back to them and use their email addresses to communicate back to them on the response that I receive from the government, or an update on that information. So while I understand your concern and the fact that you've recommended that administrative or IT staff only have the possession of those email addresses, I know the expectation that I get when I have a written petition and I submit that written petition and I get the answer back.

What I said last week at our meeting, and I'll say it again to you today, is that I think, really, we have to decide—and you did touch on it by saying "rationale, objectives and justification"—whether we have a participatory type of process, where people know at the start what they're going to get back from the government and what their alternatives are.

I still think that, regardless of what we decide, whether we decide it's a formal process through the Clerk and only IT people get the email, you're going to have members have e-petitions on their site. I still think you're going to have people that go to free petition websites and sign up, but all of them have an expectation that they're going to get an answer. So I'd be interested to see whether you have a preference. I know that you've looked at the House of Commons system and the UK system—Joanne did an excellent research paper. Do you have any comments off the top of your head?

Mr. Brian Beamish: Yes, I have a few. In terms of who should be responsible for the process, my preference would be that it be centralized with the Legislative Assembly. I think to the extent that there are different processes happening out there, the desired consistency is just not going to be there and the greater the likelihood that practices will vary and that some of the practices might not be very good.

I neglected to say it in my comments, but I'm fully supportive of the idea of citizens being able to indicate that they want to get a response back from the government. I have no problem with that at all. It can be as simple as having a toggle switch that somebody says, "Yes, I do want to hear back from you in terms of response." I think that's quite appropriate.

My preference would be to have a centralized process. I guess at the end of the day, members will do what they want to do on their own websites. I think the advice I'm giving here is as transferrable to them as it is to a centralized process run by the Legislative Assembly. I hope they would have a privacy policy in place and put limits on what they do with the information and only use it for the purposes of the petition program, and give individuals the option to hear back or not hear back. I think all those safeguards really need to be built into it.

I do think that if it is a centralized process with the assembly, the ability and the resource is to ensure that it's a secure system and proper security safeguards, encryption, audit, training—I think the likelihood is greater there that they have the resources to ensure that gets done properly.

Mr. Steve Clark: Okay. I'll let it go around. I may have another question; I know I have time remaining. So I'll let other members—I don't want to monopolize the conversation.

The Chair (Mr. Monte McNaughton): Mr. Mantha?

Mr. Michael Mantha: One of the questions that keeps coming up is the action that people are going to expect out of the petition. Right now, there really isn't a defined expectation other than an informed MPP would know that he would be getting a response and it would be up to him to transfer that to his constituents.

That action also raises a few eyebrows and concerns, for obvious reasons. One is, what is the validity that you're going to put in behind a petition? What is going to be the ask out of that petition? Really, there are some petitions that might prove to be vexatious in the making. How do you see eliminating some of those petitions?

Mr. Brian Beamish: There seem to be some good examples out there of having a screening process put in place. I think everybody understands that there should be criteria for a petition being placed on a website. Some of them are pretty straightforward: It has to be something that's within the jurisdiction of the Legislative Assembly; it can't be defamatory, inflammatory or what have you.

I think you could probably pretty quickly come up with the ground rules for what goes on and what doesn't. Then it's a matter of how you set up a screening process. That could be a committee like this, I suppose. It could be the Clerks' office itself that does that screening. I definitely agree that there should be some screening taking place and there should be some clear criteria.

I believe it's the British Parliament website that is very clear on what the criteria are on what's acceptable and what's not acceptable. It's probably a pretty good guideline there.

Mr. Michael Mantha: I just want to go back on a comment my friend brought up in regard to the varying processes. I think that may bring confusion out there in regard to actually getting that action or getting the result.

We have a process that we have in place now. It's used in two ways: first, to get one a response, but also it's a tool that MPs and MPPs utilize in order to have greater engagement with their constituents.

If we were to go to this process, and just to bring it down so that everybody is concise in regard to the

response that they're going to be getting, do you see any confusion? Actually, what we're trying to accomplish here is greater engagement. If people are anticipating getting some type of a response under one format and there's an actual other format there, aren't we creating confusion for our constituents?

Mr. Brian Beamish: I suppose it's potential. I've looked at a couple of the MPP websites and how they've operated the petition process. To be honest with you, it's not clear to me how that fits into the formal written petition, whether they gather signatures, print that off and submit that as a written petition, or, if it's not integrated into the official Legislature's petition process at all, it's a way for the MPP to gauge their constituents' views on a particular item without the expectation that it will then go on to become an official legislative petition.

There may be some confusion at that level. People may engage with the MPP thinking that this is the formal Legislature's process for petitions, when in fact it may not be.

Mr. Michael Mantha: So if we're bringing validity through an e-petition process where we're going to be expecting an action and actually expecting a response and maybe a result, would it be beneficial going with one process and one process only?

Mr. Brian Beamish: Well, I guess my views on the pluses or minuses of a single process would focus more on the privacy side of it.

Mr. Michael Mantha: Yes.

Mr. Brian Beamish: I see that as a way to manage those issues, to ensure that those issues are managed properly. I think anytime you start to defuse it and have various processes in place, it's easier that—you get inconsistency and you get a process or practices that may not be as good as they should be.

Mr. Michael Mantha: Thank you.

1340

The Chair (Mr. Monte McNaughton): Thanks, Mr. Mantha. The government now has 10 minutes. Mr. Ballard?

Mr. Chris Ballard: I'll jump in. Just wondering if, in your perspective, would e-petitions be subject to freedom-of-information access requests, and if they are, who should have access to that information?

Mr. Brian Beamish: I don't think they would be. Well, let me step back. If the process is being operated by the Legislative Assembly, they would not be subject to an FOI request. First of all, the Legislative Assembly is not subject to FOI requests for anything. Now, we can debate whether that's a good thing or a bad thing, but that's the way the law is written. The whole premise here is that other than the signatures—the petitions themselves will be available to the public, so presumably there's not a reason to put in an FOI request.

Mr. Chris Ballard: Again, just following up in terms of what information is required—great report, by the way, and it got me thinking, as you were going through there, that premise of only collecting the information you absolutely need, and that petitions aren't binding on government: So how much information do you need? There has been a lot of talk around the table about the need to verify individuals, and I suppose the fear is that a huge number of people living outside of Ontario could try and sway government policy by having hundreds of thousands of people sign an e-petition. That's a distinct possibility, but probably not terribly—probably won't be happening.

But there are jurisdictions where you sign up to sign e-petitions. So somewhere, there's a significant amount of information to verify, but then you can go in and then use that ID to sign all sorts of petitions. You can develop your own handle, that kind of thing, or the other way that you seem to be suggesting, which is simply first name, last name, email and postal code. You're happy with that. There's other ways to verify where the email comes from, those kinds of—

Mr. Brian Beamish: Yes, collecting the IP address to ensure that it's an Ontario IP address.

Mr. Chris Ballard: Yes.

Mr. Brian Beamish: I guess my fear on that is—I mean, that's definitely a solution. If at the end of the day the committee's concerned about ensuring the identity, going the extra step, that's a legitimate solution. I guess the caution is that, going back to data minimization, you're collecting additional information, which creates additional risks. The more information you collect, the more the consequences are if that information isn't managed properly. That's the caveat I would give you on that.

When I look at the paper process now, and as I understand it, it's not as if the Clerks' office takes a paper petition and starts calling phone numbers or verifying addresses. They take it at face value, right? Somebody gives their postal code and says, "That's an Ontario postal code." I'm assuming that unless there's a reason to think otherwise, they take it at face value, and I guess that was our thinking. We had some debate about whether it should be full address plus postal code, but thinking that at the end of the day the full address really doesn't add anything that the postal code doesn't give you. The postal code, if it's an Ontario postal code, you take it at face value that they're an Ontario citizen.

Mr. Chris Ballard: I just wanted to again thank you for this, because it's given me pause for thought in terms of just how much information we have to gather.

The Chair (Mr. Monte McNaughton): Ms. McMahon.

Ms. Eleanor McMahon: Excellent presentation.

Mr. Brian Beamish: Thank you.

Ms. Eleanor McMahon: A couple of questions—one of them might be outside your wheelhouse, but I thought, while you were here, if you wouldn't mind. It's Back to the Future Day, so perhaps it's in that spirit.

I'm new here, and my friend was talking about timelines. I see in the federal Parliament, in the last House, that they started looking at this in January 2014, and in committee in November of that year they were still

looking at the issues, so perhaps we're on a similar timeline.

I know that they grappled with some of the same issues that we are here as well. They talked about things like thresholds of signatures, the nature of a petition and how it would be accepted or not, and then they talked too about the need for a sponsor for that petition. I'm interested in some of these areas in terms of: Do we need a sponsor? Should we have one? Should it be a threshold of 1,000 signatures—which is one of the barometers that they talked about. Do you have any thoughts on that?

Mr. Brian Beamish: In terms of sponsorship, I'll be honest, it struck me as something that's been done all along, because that's how the paper petition process was developed. I really don't see the need for that in term of e-petitions. I think that can be placed in the hands of the citizens, to create and collect the signatures. If they hit a threshold, there's a requirement that it would go up on the website, and then there's a requirement for government action. In terms of sponsorship, I'm not sure how I see that would fit into this. I know the feds were looking at including it, but to me, it's unnecessary. I think the citizens can handle that themselves.

I think there should be a very modest threshold for a petition to be made available to the public to support or not support. I think there should be a threshold that would require some type of government action. I think it should be high enough that it's not five or 10, so that every petition requires a response, but I think it should be modest enough that people have some comfort that there is a meaning to the process.

Ms. Eleanor McMahon: A follow-up—do I have time?

Mr. Brian Beamish: I'm not sure I have a—I can't sort of pull a number out of the air, but

Ms. Eleanor McMahon: No, I just wanted your thoughts on that. That's very helpful.

One more thing—may I? I was just going to ask about the sharing of best practices amongst your colleagues across the country. Of course, because there's been this federal conversation, I wondered if your colleagues across the country, if you're sharing information on this, if it's a topic of discussion or debate amongst you.

Mr. Brian Beamish: Surprisingly not. It has not been. I'm not sure—maybe Quebec might be the only province other than one of the territories that has e-petitions. It has surprisingly not been a topic of conversation, which is unfortunate.

Ms. Eleanor McMahon: I just wondered if it might be helpful for us to secure some of their information and look at it, in terms of developing our model.

Mr. Brian Beamish: I'm not sure that there's anything out there. I believe Quebec and one of the territories have it. I've looked at the territory. It's helpful.

I believe it's Queensland that has a petition process. I thought their model was very helpful. I think the British Parliament has a very good system, as well.

Ms. Eleanor McMahon: Mr. Chair, I wonder if I could ask research to help us secure some information on both of those, if that would be okay, to help guide our conversation. Would that be all right?

Ms. Joanne McNair: You've been given—

Ms. Eleanor McMahon: The Queensland model and the British parliamentary model?

Ms. Joanne McNair: In the very first report.

Ms. Eleanor McMahon: My mistake, forgive me. I must have missed it. Thank you.

The Chair (Mr. Monte McNaughton): Ms. Wong?

Ms. Soo Wong: Thank you for your presentation. I'm just going to go back to your—I believe on the bottom of page 6, you talk about the retention of the personal information gathered, but you didn't give us the timeline, how long to keep this information. What is considered best practice? And should committees or members wish to have this information—I know the speaker after you will talk about archiving this file. What would you suggest if we have e-petitions going forward? How long do we retain this?

Mr. Brian Beamish: I would draw a distinction between the petition itself and the people who have signed the petition, because I think those are two very different questions. The petition itself could be kept forever. It may only be available for signature for a certain length of time, but there is no reason why that petition can't be kept around or archived or made available.

I draw a distinction, though, with the information about people who have signed up. I think their information should only be kept for as long as required. It would seem to me, if the system is designed so that a petition is on a website, available for signature for a certain length of time and then closed, at that point, I'm not sure there's a reason to keep the names and email addresses of the people who have signed the petition any longer.

Ms. Soo Wong: The other thing that you've identified for us is the training and the administration of the e-petition, targeting specifically IT staff. I want to push that envelope a bit more, because the training of this piece is critical, and the consequences of not properly training are also a concern for me. Much of this stuff is administrative. So my question to you is, how do we ensure that these files are protected, because you've seen the breach of information regularly—

The Chair (Mr. Monte McNaughton): Ms. Wong, you have about 30 seconds.

Ms. Soo Wong: Okay. I just want to say: How do you protect the piece about the training for staff?

Mr. Brian Beamish: Security and securing the information would have both technical solutions and what I would call administrative solutions. Things like encrypting the data while it's in transit—a person is signing up and providing their information: That's encrypted, and it's encrypted while it's sitting on a website or in a database.

1350

Then there are administrative solutions: being really clear with staff about what the rules are, who can have access to that information and who cannot have access to that information. They know that access will be audited and that there will be consequences if they have broken those rules.

I've mentioned the hospital sector as an example. The need for training there really underlines this, that it's not just when somebody comes in and gets their orientation at the start of the job, they get trained once and then go for 10 years. It has to be regular and it has to be consistent. People have to be continually reminded about what their obligations are.

The Chair (Mr. Monte McNaughton): Thank you, Mr. Beamish. We'll go back to the official opposition. You have just over four minutes.

Mr. Steve Clark: Mr. Beamish, I agree with your conclusion that e-petitions do have the potential to improve the quality and level of engagement of Ontarians. It's really the media they use today, and I think that's—the feedback that I've gotten from a number of folks who have gone ahead on their own, set up their own e-petition, gotten 35,000 signatures and then were shocked when I had to print them out and get one person to sign it to table it in the Legislature for them to get an answer. So I think your comment about action is probably the key thing that this committee has to deal with when it starts report-writing in November: What type of action do we want out of this policy?

Just above your conclusion, you talk about the privacy impact statement, or PIA. I'm just wondering, how long do you think a PIA on e-petitions would take this committee? Would it be a month? Would it be two months? What would you think would be reasonable?

Mr. Brian Beamish: If this committee recommended that a PIA be done and that that task be given over to the public service, to the Ministry of Government and Consumer Services, which would be the logical route, I don't think it would be a lengthy task. I know you're going to have Mr. Roberts up next after me, who could probably give you a more definitive answer. Maybe I'm being naïve; I see this as a fairly relatively straightforward process. The issues are clear and it's a matter of finding what the right solutions are. I would assume it could be done within a month or a couple of months. But as I say, Mr. Roberts is up and maybe will help you.

Mr. Steve Clark: I look forward to Mr. Roberts finishing that answer when he—

Mr. Brian Beamish: And I would like to emphasize that, again, my office would be happy to be a resource on that, which may help speed the process up.

Mr. Steve Clark: That's all.

The Chair (Mr. Monte McNaughton): No further questions from the official opposition—

Mr. Brian Beamish: Now that I've set the standard for Mr. Roberts, I can—

The Chair (Mr. Monte McNaughton): Well, Mr. Beamish, on behalf of our committee, thank you very much. That was a great presentation.

Mr. Brian Beamish: Thank you very much.

OFFICE OF THE CHIEF PRIVACY OFFICER AND ARCHIVIST OF ONTARIO

The Chair (Mr. Monte McNaughton): Next we'll hear from John Roberts, the Chief Privacy Officer. Mr. Roberts, you'll have 30 minutes for your presentation, and then each party will have 10 minutes to ask questions after. Thank you.

Mr. John Roberts: Thank you very much. First of all, I would very much like to thank the committee for the opportunity to provide some remarks this afternoon, wearing both my hats as Archivist of Ontario and Chief Privacy Officer. The issues that you're considering have implications across both the information management, privacy and archival aspects of my division's work.

It's great to see the deep thought that's going into those aspects through the committee's deliberations. In reviewing your transcripts of the hearings over the past few months, I was struck by the range of perspectives that have been brought to bear and the thoughtful consideration and deliberations that have been going on, and the range of resources that you've already considered.

I know that you have looked deeply and widely into the subject, so the remarks I bring today will probably not cover a lot of new ground for you, and indeed will echo much of what Commissioner Beamish has just presented. In part, I think that's a reflection of the fact that privacy practice is now an increasingly mature discipline, with good practices fairly well established and at times quite well structured in methodologies, like the PIA, the privacy impact assessment piece that was mentioned previously.

I'm delighted to bring my perspectives to bear and to reiterate the importance of giving really significant consideration to privacy issues. From a public service perspective, we now have a meaningful, good consideration of privacy issues in terms of maintaining public trust and confidence in the workings of any organization. So I commend the fact that you're taking the information management and privacy considerations of a shift from paper petitions to e-petitions very seriously. Certainly, for me, with Chief Privacy Officer in my job title, it's incredibly heartening to be providing some evidence to a group who are very much already on board in taking the issues seriously.

Perhaps the key messages that I'd like to leave you with right up front: Firstly, when looking at the best way to deal with privacy concerns, it's important not to simply automate an existing process but to actually reflect on what the requirements are for the process to work effectively in a digital environment. That's both around managing the risks as well as optimizing the benefits that can be gained. Again, there are clearly huge benefits in terms of openness engagement from moving to an e-petitions environment.

Secondly, I'd like to emphasize that, in developing a privacy-protected solution, it's not just about the technical solutions or the application or the website interface; it's very much around what I would consider the privacy ecosystem that's at play. That's around the culture, it's around the training, it's around the processes as well as the technical solutions that are in place. So I'd urge you to think widely about the mechanisms and interventions that are available to build a strong privacy solution.

Finally, I'd like to also note that there are methodologies, as I said, to complement the evidence that you're hearing from multiple witnesses. I would certainly endorse Commissioner Beamish's recommendations to go through a privacy impact assessment statement, and would certainly offer the support from my division to work with the committee or with the Clerks to help you through that as a systematic approach to understanding what the real and potential privacy risks are and developing mitigation strategies to deal with those.

By way of background, I am, as you can tell from my accent, not a native Ontarian. I'm just a month into my job as Chief Privacy Officer and Archivist of Ontario, coming from a role in New Zealand where I was working with the national archives of New Zealand for around 20 years, and more recently alongside the Government Chief Privacy Officer in New Zealand and dealing with many issues of service transformation and the digitalization of services. I'd like to bring a few of my reflections as well as the experiences that we have in the information, privacy and archives division. As I mentioned earlier, you will find that many of my remarks echo the comments that Commissioner Beamish made just previously.

I would note that privacy principles are generally technology-independent. The principles of maintaining privacy, of informed consent, minimizing the amount of information to be collected, maintaining it only for as long as it's needed—those are principles that are valid whatever format is being used for the conduct of business.

It's also worth noting that there are some very real changes that occur when shifting from a paper environment to digital. One of the key changes is the loss of what's called "practical obscurity," a phrase that Mr. Beamish mentioned previously. In paper, a process can be open, but require someone to actually come to the Legislative Assembly buildings and inspect documents that are public. In a world of Google search, if those documents are equally public, then a simple search on a Blackberry or on a phone can sometimes reveal information to the prurient searcher rather than to the person with genuine interest in locating information.

Equally, the risks associated with inadvertent release or sharing are that much greater. Taking a potentially very large submission and inadvertently stuffing it into an envelope and sending it to the media are almost null. The risks of inadvertently sending a very large digital file as an attachment are that much greater because of the ease of transmission. The very characteristics that make digital information so simple and effective to use—the ease of copying, the ease of distribution, the ease of publication—are those that give rise to the greater risks. So, while the processes may be similar, there is a need to consider where those risks or the impact of a breach may be that much greater.

In my role as Chief Privacy Officer and Archivist, I lead the division that supports the Minister of Government and Consumer Services in carrying out his duty, but also supporting the broader public sector and the Ontario public service around many of the issues that you're considering: developing policy advice, training, building communities of practice, supporting the regulatory environment that operates within government, and advising the OPS around privacy issues.

1400

I'm very mindful of the fact that the Legislative Assembly is not subject to the Freedom of Information and Protection of Privacy Act or to the Archives and Recordkeeping Act, so I'm very cognizant that I offer my comments today purely in an advisory capacity. Hopefully there will be something from the observations and the experiences that we've had within government that is of value.

I'm also appointed by order in council as Archivist of Ontario. I know there was some interest in some of the records retention questions earlier, so I will offer a few remarks just about how records retention can be thought about and the implications and approaches to managing e-petitions and their relationship to the provincial documentary heritage record. Clearly, there's a trade-off around managing historical resources but also protecting privacy. Part of the role of my division is to help those trade-offs be made effectively.

It's critical that we are very careful and prudent in terms of managing public information. It's clear that there's also a huge upside that can be gained. From listening to your comments early this afternoon, I don't need to reiterate the point that there are genuine benefits to be obtained in terms of the relevance, the accessibility and the openness of the process through allowing e-petitions. It is the channel through which people engage in their day-to-day lives with business and with government. Many, no doubt, would like to engage through those same channels with the Legislative Assembly. I won't emphasize that point any longer. Suffice it to say, there are clear upsides to a shift of technology, but as I've mentioned, there are also risks that need to be managed.

Personal information is intrinsic to most interactions. The process that you have for petitioning clearly does create and capture personal information: names, addresses, and, at present, signatures. The question is not whether personal information should be collected or whether there are privacy issues; it's how much, how it's created, how it's captured, and how to manage those issues.

The process that we use, as has been mentioned, within the OPS for working through, in a methodical way, the risks and issues is what's called a privacy impact assessment. So whenever there is a change in a program or a change in a process that leads to changes in the way information is collected, used, disclosed or created within government, there's an obligation to go through that process. As I mentioned, I respect that that obligation does not apply to the Legislative Assembly, but I would strongly urge you to consider taking that approach, which does reflect international best practice as providing a methodical way of working through a

range of issues, and probably corralling the evidence and the issues that you've been debating and discussing with various witnesses over the past months.

It is an analytical process involving a set of activities and a set of deliverables; it's not a single document. It's designed to help identify, address and document the issues, quantify the level of risk associated with them, and understand the mitigations that could be put in place to address those—so, really, to help with the detailed design choices that any program will need to go through as it gets closer to an implementation phase.

Ideally, that sort of process should be undertaken as early as possible in the life cycle of an initiative, once there's a broad sense of what's going on, but ahead of too many decisions having been taken around the actual design solutions—because it is a good mechanism for flushing out different ways of resolving questions rather than leaping to conclusions.

My division does have a range of guidance available. As I said, I'd be more than happy for my staff to work through with the committee, or the committee Clerks, the details of that.

There was an outstanding question around how long that process might take. My view is that it would be probably eight to 10 weeks for an initiative of this sort, given what I've seen in the transcripts and my understanding of the process. As Commissioner Beamish said, it's not an unduly lengthy process but one that does give an opportunity to work through and make some decisions around how to manage trade-offs about accessibility versus protection and the like.

Another process that I would like to mention and suggest be undertaken is called a threat risk assessment. This relates to the interplay between security and privacy issues. In many cases, privacy breaches occur where a system is hacked or where there is an attack on it. That represents not necessarily bad privacy practice, but shortcomings in the security of the environment and the application. A process known as a threat risk assessment provides a complementary mechanism of looking at what the security arrangement should be in an online environment. Again, there is guidance available from OPS colleagues around how that would work. We can help you understand not just the privacy practices, but how to build an environment that would be secure in maintaining those practices over time.

In providing some further comments on privacy issues, I'd like to look at four broad processes: collection; disclosure and use; management and protection; and retention. Because when we think about the information life cycle through a business process like petitions, those, to my mind, are the four key areas that deserve a level of consideration.

If I can talk firstly to the idea of collection—again, Commissioner Beamish mentioned a number of times the principles of minimizing the amount of information that is collected. As I commented earlier, I'd urge the committee not to simply replicate in your e-petition process all the data, all the attributes that are being currently collected in paper form. Having looked at your previous deliberations, I know that you're very mindful of the fact that changing technology platforms means different information is probably necessary. That's not only around minimizing the privacy risk by minimizing the amount of information, but also there's a key privacy principle around informed consent.

It's important to enable people who are participating in a process and providing their personal details to understand what will be done with those and how they will be managed. One of the phrases that's used in privacy practice is called "notice of collection," a statement that will advise very explicitly people who are providing personal information, what will happen to it; who will have access to it; under what conditions it may be disclosed; who will be able to search it; the length of time for which it would be retained and the like. Again, that sort of approach helps build public confidence in the process by making it very explicit what is going to be done with the information they are providing. It helps build that confidence in providing the information.

It's critical to think when collecting information of what the actual purpose is for which it is being collected: Why do you need address information, and which details will suffice for that? Again, I'm reiterating Commissioner Beamish's words: If the intent is to validate that someone is a resident within the province, what's necessary to achieve that? Is it simply an assertion by the individual that they are a resident, or is it further details such as a valid postal code, a full address—what level of information is required? The underlying principle being, collect only that information that is necessary for the purpose. The privacy impact assessment is to help people think: What is actually the purpose, rather than making assumptions about the intent.

If you do go down that notice of collection path: clear, plain English language is critical to make people comfortable with it; the intent being to develop trust and confidence. A process that says, "We're going to collect information," but then obscures what will actually be done with it through legalistic jargon is unlikely to achieve the intent. My staff can help with examples of good practice around what notices of collection would look like.

There are also technical considerations such as email addresses, IP addresses and the like. Again, I won't repeat what Commissioner Beamish has said, but there are, as well as the data that can be provided by individuals, data fields that can be collected automatically through the interaction online. It is important to think about those as well as the data provided, and to be very visible and explicit about what information is being captured in a machine-based way from the interaction and making that known, too, and ensuring that that is properly managed in the overall solution.

1410

The second core area I'd like to talk about is disclosure and use of information. It's one thing to collect the necessary data, but to whom will it be available, how and when? Again, the digital environment offers an opportunity to decouple which information is presented

to whom in some quite significant ways. A paper petition has everything largely locked in because of the technology, because of the constraints of paper. In a digital form, it is very easy to manipulate it, to redact it so that certain participants only get access to certain fields of information, whether that be through what's available to search online or to various participants who need to administer the process. So there's an opportunity there, through deliberate, considered design, to make sure that not only is the information that's collected at a minimum but only a subset of that might be presented to individual actors or agents through the process, again to minimize the privacy risk of misuse.

What's available online for people to search is clearly a key consideration. I think that lens of practical obscurity is a very valuable one to use in the sense that information may be a necessary part of the process for transparency of the petitioning mechanism, but that doesn't mean it all needs to be available for search online.

Equally, where information should be made available to ensure that legitimate public interest in the accountability is served, how can that be made well and easily available in line with some of the thinking of open government and open information—not just publishing but publishing this information in a way that can be reused by others through the formats that are chosen, through the way that the Web interfaces are designed to enable the legitimate purposes to be easily and efficiently served, to enable the formal Legislative Assembly Web presence to be reused and interoperate with other online initiatives as part of the overall Web world.

The more available information is, of course, the greater the risk of identity theft or fraud or misuse. So with most of these privacy issues, it's not that there is a right way and a wrong way. There's a balance to be struck between visibility, accountability and transparency and protection, security and privacy. Processes that are very tightly controlled and restrained may be difficult for the public to access and effectively undermine the intent of opening up an online channel. They may make it difficult for others to scrutinize the process or to see what's happening and get involved. So a balance needs to be struck at all times between the intent of open, visible, accessible government and secure, protected, privacy-aware government.

The underlying principle in terms of disclosure and use in the Ontario public service and under FIPPA is that information should only be disclosed to support the purpose for which it was originally created. In that sense, I'd urge the committee to take a relatively broad interpretation of that so that the purpose is not simply to adjudicate on a particular petition but also to manage the integrity of the petition process and the confidence in government as a responsible organization over time. But it's a good lens to think what information should be made available, to whom and how—in practical terms, the sorts of approaches that lead to those that you've been discussing, that an online portal may only disclose the name of the original petitioner, potentially the sponsor, rather than all the signatories, to protect their privacy. So there is a range of mechanisms available there.

From the earlier questions, I did hear some interest in the issues of retention and how long information might be kept. The general principle here again is to collect and retain information for as long as it's necessary for the purposes for which it was originally collected. But again, I would urge the committee to consider that in a broad sense, that it's not simply to retain the information until the particular petition has had a response but to think about the integrity and transparency of that process over time.

Early disposal by destruction of information is a practice that I've seen recommended in a number of the regimes that you've been looking at. Clearly, that is a very strong way of protecting privacy, by destroying the information to prevent any further potential for misuse, breach or leakage.

If I can put my Archivist of Ontario hat on just for a moment, I'd also note that petitions to Parliament are, in a way, a key part of the record of society's interaction with policy-making and legislation-making at the highest level. The Archives of Ontario are certainly very used to maintaining, with high levels of protection of privacy, records of government over time so that they can serve as part of the documentary heritage of the province.

Now, I haven't formed any particular view on whether the full, detailed petitions should be kept in the long term/medium term. I do note that from my previous life in New Zealand, some petitions with personal information around signatories have formed really valuable historical resources. The prime example from New Zealand was the petition for women's suffrage. New Zealand was the first country in the world to grant women's suffrage, and now it is a great source of pride for people to find their ancestors as signatories to that petition. I bring that just as an example of how the rich personal information included in detailed petitions can, at times, also serve a documentary heritage and a national or provincial identity purpose, as well as the narrower administrative governance process.

At this point, I'd simply urge the committee to make a considered recommendation around that issue and to recognize that there are many ways of skinning a cat, if you like, around the protection of privacy long term. My institution would certainly welcome ongoing discussion around what the right approach would be in that area.

A final area of issue I'd just like to talk about is the management and protection of the information. So having collected it, it's critical that that data is stored in a way that will manage the privacy and avoid undue risk to its disclosure or misuse.

That takes us to two areas: Firstly is the question of security, as I mentioned previously, with the mechanisms around threat risk assessment. A well-designed system can still cause great privacy harm if it is subject to security breaches or to hacking from outside. So a robust security consideration is one of the ways of managing that. Again in technical terms, that goes to things like

data encryption, the level of password protection, access to the system and the like.

The second area, in my view, that's equally critical is that broader ecosystem within which the system is operated, questions of culture, training and behaviour. Different people need to be involved in administering a technology-based system than a paper-based system—IT administrators and the like, potentially even outsource providers. So it's important there to maintain the integrity of the overall system to look at the right level of policies, the right level of training, the culture that need to be installed, and people who may be new to handling of this information, to make sure that they respect the sensitivity of the data that the public have entrusted to you and are able and aware of the challenges in managing it—so not simply a technical approach, nor indeed even a policy approach.

The IPC, I know, has a resource with the wonderful title, A Policy Is Not Enough: It Must Be Reflected in Concrete Practices. So issues of training, privacy awareness and privacy maturity are a key part of that, as well as practices around the response, should there be a privacy breach. The best system in the world is still going to have some risks that it could be hacked or that people could act negligently or just in error. Human error is one of the biggest grounds for privacy breaches. Organizations are often judged not by the fact that something went wrong but by their response.

Again, as part of building an overall approach to a privacy-smart e-petitions process, I'd urge you to look at the remedies and the response mechanisms should something go wrong, should information be inadvertently misused.

1420

That importance of training awareness maturity would need to be applied to all actors in the system. Beyond those who currently have a role to play in respect of petitions, as I said, when a process is automated, when it's put into a technology environment, there are a number of other parties who necessarily have a part to play, typically the more technology or system administrator-type roles.

In order to do their job, in order to keep the system running, performing, they need access at some level to the data. There are protections that can be put in place around encryption, but there are new risks that come into play as new actors get involved in the ecosystem.

Just in closing, I don't think I've really brought much new to the table for you, but you've been looking at this issue for some time and may try many different perspectives to bear. The ground is reasonably well trodden in terms of automation of a business process. There are some standard mature practices to apply. I think there are huge benefits to be gained from putting in place a petitions process that is more accessible to everyday Ontarians, but the risks that go with that do need to be managed.

I'd like to again offer the support of my division as you work through the details, and thank you for the opportunity just to provide these comments this afternoon.

The Chair (Mr. Monte McNaughton): Great. Thank you very much, Mr. Roberts. We'll begin with the third party and Mr. Mantha, if he has any questions.

Mr. Michael Mantha: Thank you, Mr. Roberts. I do have to say that your presentation was very detailed. As you made your presentation, you were answering several of my questions, so you did a great job. As you were going, I crossed off the two. Anyway, thank you for your presentation.

The one question I do have is more of a hypothetical question, particularly with your background and your field. I want to go back to a question that my friend Mr. Clark asked. The scope of a privacy impact assessment on this process is eight to 10 weeks. Within those eight to 10 weeks, hypothetically, what could cause an extensive delay in making that assessment? Everything is going fine; everything looks good. But what would a delay look like? What could that possibly be?

Mr. John Roberts: What could cause a delay in that process? A significant information gap around a key input; for example, if there were no sense of Ontarians' desires or sensitivities in the space.

As I said, these processes are largely around balancing multiple interests, so if there is no input around one of those key stakeholder interests, it could mean that some additional research would be needed in order to balance the factors.

My sense, from what I've read of the committee's deliberations and from the various other jurisdictional reports, is that those factors are relatively well understood. So I think it's unlikely, but it's difficult to make any kind of trade-off decision or risk management decision in the absence of solid information.

Mr. Michael Mantha: Okay. Let me throw this at you: Could one of those delays within the impact assessment—because we've seen—at least, I'm hearing that there's a different view in regard to the result that we want to see at the end of an e-petition—the goal, the objective, an action. Could that be a substantial delay in moving the impact assessment forward?

Mr. John Roberts: If there is no clarity about what the subject of the impact assessment actually is, then yes. If there are wildly different views as to what the nature of the process would be—what an e-petitions model would look like—that could make it a lot harder to operate, because the scope is indeterminate.

Mr. Michael Mantha: Yes. I'll pass it on.

The Chair (Mr. Monte McNaughton): Okay. Thanks, Mr. Mantha. Mr. Ballard?

Mr. Chris Ballard: First, I had a question on process, Chair. We have our table research clerk, who I imagine will be coming back with a draft report. I've heard both gentlemen today say that they would have lots of information for us. That's not the process? I'm seeing some heads shaking.

Mr. Steve Clark: No.

Mr. Chris Ballard: How does the process come back, then?

Mr. Steve Clark: At the end of today, after we're done, I'm going to ask the question: Is the government going to table a discussion document?

Mr. Chris Ballard: Okay, perfect.

Mr. Steve Clark: Or are we expected to develop the framework by consensus?

Mr. Chris Ballard: Okay, that was where I was going.

Mr. Steve Clark: That's the question I'm going to ask the government.

The Chair (Mr. Monte McNaughton): Mr. Ballard.

Mr. Chris Ballard: Thank you very much. I have the same issue. I had six questions here that I was going to ask you, and as you spoke, I was able to check them all off. I really appreciated the depth of knowledge you're bringing in.

I have some sense of how the archives store and treat paper documents. How would you be treating electronic records for the future? Can you just walk me through a scenario: How might electronic records, electronic petitions, be kept for future access? I'm back and forth in terms of how much information we attach to it.

You raised the historical concept for researchers, which I think is probably now a little more important. I guess you were thinking more of the archivist, when you were talking like that, than I was thinking privacy: Don't leave too much information attached. Can you walk me through how you would see electronic documents being stored?

Mr. John Roberts: There's a huge body of literature on the practice of electronic archiving, obviously, which speaks to things like the integrity of the document. Digital forensics and those disciplines have brought a lot in terms of ensuring that a document is unaltered over time. There are technical mechanisms for making sure that documents remain unchanged over time. They are put into a secure environment where there is controlled access in terms of who can access them.

From a long-term preservation perspective, understanding the data and the document formats is critical to understanding when they might become obsolete and ensuring that there are then highly trustworthy migrations in place.

Paper has the advantage of being very stable. You can go back to petitions from the last century and read them and understand what's going on. I think we've all got experience of looking back at digital information from even 10, 20 years ago and getting that "unable to open document" message. So a more active regime is required, from a preservation perspective.

The protections can be largely reflective of the protections that were put in place during the active management of the records—security; access permissions. You'll all be familiar with document management and online environments where there are quite complex and strong permissions regimes that allow only certain individuals to access certain documents and files—those kinds of techniques, applied within an electronic archive, to maintain the trustworthiness and avoid misuse of information that is stored.

Accessibility is another challenge with digital archives in terms of just how they then get surfaced and used by the public.

Mr. Chris Ballard: Can you even offer up a ballpark figure, from a retention perspective, about what this might cost?

Mr. John Roberts: From a retention perspective, the petitions would just be one strand of documenting the digital heritage of the province. I would caution against any bespoke or particular retention solution for e-petitions and treat it as one set of documents that have long-term value that need to be managed, as do many public digital records that are currently being created. I would say that it's not a material new cost. It's just another part of the province's documentary heritage in digital form.

Mr. Chris Ballard: Okay, very good. Thank you.

The Chair (Mr. Monte McNaughton): Ms. Wong?

Ms. Soo Wong: Thank you for your presentation here today. I'm going to go back to Mr. Ballard's question to you.

I want to know, because this is electronic, do we have the correct mechanism in terms of software and the ability to do the archives that you're asking us to consider?

Mr. John Roberts: At the moment, we have some limited capacity, and we're working with the federal government on robust, industrial-strength solutions. Globally, digital archive solutions are still in their relative infancy. Ontario is no better or worse than almost every other jurisdiction that I'm aware of. It does have capacity for managing digital information. It probably doesn't have a 20-year solution yet in place.

1430

Ms. Soo Wong: So to bring that to the industrial one that you're suggesting to the committee, how much would that cost?

Mr. John Roberts: That's a matter that we are partnering with the federal government on. I haven't yet seen a business case or a sense of where the funding streams are. That's something that is high on my to-do list, arriving in Canada. Systems, internationally, vary in cost, depending on the risk appetite of the individual organizations.

Basic digital archiving capability, which relies more on the competence of the individuals in leveraging enterprise IT capability from within government, is relatively cheap. They're essentially leveraging secure file storage environments that are already in play. Dedicated digital preservation environments can cost in the low millions of dollars. But what's right for Ontario is still—

The Chair (Mr. Monte McNaughton): Ms. Wong, you have just over three minutes.

Ms. Soo Wong: That's it. I'm done.

The Chair (Mr. Monte McNaughton): Okay. Any other questions from the government side? We'll move to the official opposition. Mr. Clark.

Mr. Steve Clark: Thanks, Mr. Roberts, for your presentation.

I guess one of the things that I wanted to put forward—we should mention the PIA, the privacy impact

assessment, would take about eight to 10 weeks. Mr. Beamish talked about the Ministry of Government and Consumer Services having a document. I wondered, between you or Mr. Beamish, whether the committee could have that document tabled with us so we could get an idea of the tool that's available right now.

Mr. John Roberts: We can provide that shortly after—

Mr. Steve Clark: That's great. If you could provide it to us, that would be great.

Mr. John Roberts: —there's a guide from Mr. Beamish's office and some further material from my division.

Mr. Steve Clark: So we develop a framework, I assume, at the committee level. We go through the PIA assessment. Then you recommend we'd go through a threat risk assessment after that?

Mr. John Roberts: That could be done in parallel with the privacy risk assessment. That's understanding the threat environment from a security perspective. As I said, privacy and security don't go hand in hand in terms of the actual risk involved.

Mr. Steve Clark: And both you and Mr. Beamish—both your offices could provide resources for that threat risk assessment?

Mr. John Roberts: It's a different branch within the OPS that has the detail there. I know there is plenty of guidance available and I'm happy to work with the committee to help access the right insights to go through that process as well.

Mr. Steve Clark: But just to be clear, you don't perceive that that threat risk assessment would delay the process? We could do it in parallel over that eight-to-10-week period after we develop the framework.

Mr. John Roberts: I believe it could be done in parallel. Yes. That's my view.

Mr. Steve Clark: I'm just looking at a runway to come to some resolution and some path forward. We still have to, no matter what changes we make, get the government House leader to actually agree to have the standing orders changed. Presently, the petition system only deals with the paper petition.

You made a comment that spurred on a question. I stand up in the Legislature and I have my stack of 8.5-by-11 pieces of paper with all the signatures on it, and I read it into the record and I give it to the table, and the table gives me an answer. Where does that petition go? Do you then archive that entire document somewhere?

Mr. John Roberts: Current arrangements—the Legislative Assembly is voluntarily archiving that material with the Archives of Ontario—

Mr. Steve Clark: For how long?

Mr. John Roberts: We are currently holding those in perpetuity.

Mr. Steve Clark: Oh, my God.

Mr. John Roberts: Subject to—as I said, part of our core competency is to protect privacy, so they are kept in secure facilities and not made available without the privacy—

Mr. Steve Clark: The actual document?

Mr. John Roberts: The actual documents, in the current arrangements, are being held as part of the documentary—

Mr. Steve Clark: How big a facility do you need to store all those petitions in perpetuity?

Mr. John Roberts: To be honest, the inputs that we get from the Legislative Assembly are a relatively small part of documenting the activity of government as a whole. We have, at the moment, over a million and a half boxes of material stored in one form or another.

Interjection.

Mr. Steve Clark: Well, this is even more reason why we need to develop a framework at this committee to move this forward.

Mr. John Roberts: With my archivist hat on, some of the efficiencies around long-term storage from shifting from paper to electronic are appealing.

Mr. Steve Clark: I guess the last question I have is about your comment about informed consent. Do you believe—and if Mr. Beamish has a comment as well—that all MPP sites should have a section that communicates to constituents how we gather information on that site and what we use it for? I don't see that consistently being applied amongst all the MPPs. You're here, so I might as well ask you for a comment on that.

Mr. John Roberts: What I would say is that it is good privacy practice to advise people who are providing personal information what will be done with that information over time. So most of the privacy methodologies that you would see typically in public administrations do urge that there is clarity around how the information will be used, disclosed, managed and the length of its retention.

Mr. Steve Clark: Thanks very much.

The Chair (Mr. Monte McNaughton): Thank you.

Mr. Mantha, you had some time left.

Mr. Michael Mantha: I had some comments just on the last discussion that came up. You talked about the four principles of collection: disclosure, management and protection; right?

Mr. John Roberts: And retention.

Mr. Michael Mantha: And retention—I forgot that one. That's where my question is, on retention.

Mr. John Roberts: It was the fourth one.

Mr. Michael Mantha: I just want to make sure that I got this right. From your experience that you had in New Zealand, someone had the ability to go back into the archives and find Mom's signature on a petition that she did while she was in her college days, which was significantly 50 years ago.

Mr. John Roberts: That petition that I mentioned was from 1893.

Mr. Michael Mantha: 1893?

Mr. John Roberts: 1893, yes.

Mr. Michael Mantha: It wouldn't have been my mom—

Mr. John Roberts: Particularly around the centenary of that petition, there was an upsurge in public interest, and it did bring to the foreground the way in which records of people's ancestors participating in ground-

breaking public policy was something that individuals took great pride in. So I offer that just as an example of how personal information can have a long-term heritage value, as well as bringing into play privacy risks and, therefore, the need to make a balanced consideration as to what's kept and for how long.

Mr. Michael Mantha: It was the point that I was going to make, because I know my friend here was just trying to stress a point of why we need to push these as well, but those paper-copy petitions today are a paper copy, but they might have historical significance and we have to possibly maintain that practice, as well as an electronic copy.

Mr. Steve Clark: Well, you couldn't do the same thing you did in New Zealand.

Mr. John Roberts: Equally, I'd suggest that in parallel with considering e-petitions, then it might be timely to revisit the discussion around paper petitions and ensure that you've got a harmonized regime in place, so the analysis that is done of the value would be equally relevant across multiple formats.

Perhaps just one final remark: In New Zealand we did find that there was a lot more public use of that historic petition when it had been digitized and put online. Again, just as I indicated, the accessibility of resources when they're in the Web environment is substantially greater than it had been.

Mr. Michael Mantha: I asked this question earlier to Mr. Beamish and I'll ask it of you as well. The goal that I think everybody's agreeing to in this room is that we want to see greater participation and greater transparency. Do you see a conflict between having two different systems or possibly three different systems or do you see greater transparency, greater participation when there is one method: This is the method that will be recognized.

If this committee agrees on a goal, an objective and a directive that this is the method that we're going to use, and there are different methods of bringing a petition forward, do you see confusion that is going to be happening? Do you see a potential for a breach of privacy that might happen?

Mr. John Roberts: My experience in New Zealand around moving different business processes online suggests that there's great participation when actually a range of different channels are offered. There will always be people who prefer to use a familiar paper environment rather than a single channel.

1440

My experience, and the research that I'm familiar with from New Zealand, suggests that if the goal is maximum participation, then that's not compromised by having multiple processes available.

M. Michael Mantha: C'est bon.

The Chair (Mr. Monte McNaughton): Thank you, Mr. Roberts, for your presentation today. It's very useful. Thank you.

Ms. Soo Wong: I have a question.

The Chair (Mr. Monte McNaughton): Okay. Ms. Wong.

Ms. Soo Wong: Thank you, Mr. Chair. My question is, through you to the Clerk—I remember, in a subcommittee, we identified two witnesses for today's session, and the Clerk was supposed to get back to the committee on whether we were successful getting hold of the speakers for next week. So I just want to get an update from the Clerk about those other witnesses that we have asked to be presented to this committee—or we could do a teleconferencing.

The Chair (Mr. Monte McNaughton): Sure.

The Clerk of the Committee (Mr. Trevor Day): Okay. In response to your question, in the subcommittee report that was adopted, point 1 said, "That the Chair of the committee invite the following"—Mr. Beamish and Mr. Roberts.

Point 3 was, "That the table research officer provide an update ... and establish an appropriate contact in both Houses for further inquiries."

The committee didn't actually adopt bringing those people here. We said we would set up contact with them and attempt to answer any questions that the committee members would have.

Ms. Soo Wong: Okay.

The Chair (Mr. Monte McNaughton): On that note, I would like to ask the committee and get some feedback.

Point number 4 said that the committee begin in camera report-writing on November 4. We have nothing scheduled for next week. Do we need to have a meeting next week?

Mr. Steve Clark: I guess, Chair, I'd go back to what I said earlier when Mr. Ballard mentioned—we need to understand that there are some issues that have to go around the standing orders, and some changes.

Let's face it: This government has a majority on this committee. To use a term that my colleague from Lanark–Frontenac–Lennox and Addington used many times when we first started this discussion, I don't want this committee to be frustrated by going through a scenario that leads nowhere. If the government has a preferred direction on how they want to move forward with the framework, they should table it with the committee, or, if this committee is going to be allowed to develop the framework by a consensus position, then we need to understand the positions of all three sides.

Mr. Balkissoon is looking at me, because we have sat here in this committee and dealt with standing order changes that went nowhere. I really do believe we need to have an idea from the government on how they want to proceed.

I can continue to go with the e-petition that's on my site. I can communicate to my constituents how I'm going to manage their data.

I do believe that Ms. McNair tabled some exceptional documentation before this committee. I want it on the public record that I was excited about the UK petition site, and as most of you know, I don't get excited too often.

Now Bas is laughing.

I think we need to move forward. But, listen, the government has got the majority on this committee. I'd

like to know where they stand and how we move forward. If that's what we do next week—receive a document from the government and then go into report-writing—I just want to move forward. You guys know where I stand. I want to get moving. I'm doing it, my constituents are doing it, and I just think we need to legitimize the practice.

The Chair (Mr. Monte McNaughton): Any other comments? Mr. Balkissoon.

Mr. Bas Balkissoon: Mr. Chair, I come and I sit on this committee, and we've gone through this exercise. Mr. Clark seems to feel that maybe we have a position. I don't believe we do.

We support e-petitions. The problem I'm having is that maybe we need to spend next week and just kind of go around this. Mr. Clark has a position of his own on what kind of e-petitions he likes, which is similar to what he runs out of his office right now. I think Mr. Hillier had another position.

What we've heard from the majority of expert witnesses—I think the majority are causing me to hedge toward the Legislative Assembly, under the Clerk's administration, that you have a general petition, that the general public can start a petition and we develop the process, how it will go through the system, get answered and whatever.

So I think, amongst ourselves—and this is just my personal position—we need to have a discussion and land on one, and then we write the report on that. If we don't land on it, then we have to write a report saying what we heard, what Mr. Clark's position and Mr. Hillier's position is, and send it back to the assembly.

Mr. Steve Clark: I'm quite willing to build on consensus, but let's face it: You've got your majority on the committee.

The Chair (Mr. Monte McNaughton): Sorry. Ms. Wong—

Mr. Bas Balkissoon: But e-petitions are to serve the entire Legislature; it's not to serve the government only. I'm open-minded. I'm going to look at the practicality of it, the purpose, what it serves and what the public gains out of it. That's my comment.

The Chair (Mr. Monte McNaughton): Great. Thank you.

I just want to get some direction as to whether we have a meeting next week, and if so, what's on the agenda. Ms. Wong.

Ms. Soo Wong: After the Clerk clarifies what we, as a subcommittee, decided, I don't think I've heard from the members here today that if we have any questions—remember? I just heard that any questions members have to be forwarded to the House of Commons or the UK—I didn't hear a response. So maybe it is appropriate to have a meeting, or if we don't have a meeting, by this date, this time, we submit the question to the Clerk so that he can—because that's what I heard, right?

The Chair (Mr. Monte McNaughton): There were some questions, and the Clerk just passed out the responses now.

I think it sounds like we should have a meeting next week, so we'll put an agenda together.

Mr. Ballard.

Mr. Chris Ballard: Just a question and maybe a request of our research clerk—and it was sort of where I was going before. From the two gentlemen today, what I heard was that they're willing to help us in some critical areas. But what I'm wrapping my mind around is the decision points. We do one, two, three, and the subset of three is this—almost a decision tree or something like that. I'm not too sure if it's possible to dig down and get back to us with what those key decision points are in putting a system together, because I heard "You should consider this, you should consider that, you should consider this"—I'm scrambling to take notes. I'm not sure if you can help us—because it would help me.

Ms. Joanne McNair: I can certainly attempt to put something together.

Mr. Bas Balkissoon: A summary.

Mr. Chris Ballard: Yes, just a summary. I'm not looking for pages and pages, but what—

Ms. Joanne McNair: Like a flow chart?

Mr. Chris Ballard: That would even help. You know what? That might even be easier. Just what the key decision points are in terms of designing a system.

Ms. Joanne McNair: Okay. Obviously, it's going to be a purely hypothetical system because I have no idea what you—

Mr. Chris Ballard: Absolutely. No, it's up to us to decide on a system.

Ms. Joanne McNair: —where you wanted to go and stuff, but certainly I can put together, based on what we've heard and what other jurisdictions are doing, the best practices and what steps need to be considered.

Mr. Chris Ballard: If you want to do a nice flow chart picture, that's perfect, whatever.

Ms. Joanne McNair: I can try to do a flow chart, yes. I love charts.

The Chair (Mr. Monte McNaughton): Mr. Mantha.

Mr. Michael Mantha: Maybe Joanne or the Clerk can help me out here. I just want to make sure that I'm—if I am to understand, we are in favour of proceeding with an idea of e-petitions, is what I'm hearing around the table. It is how that's going to be done. Mr. Clark is indicating that he'd like to have the process that we have now, which I have on my website too, as well—

Interjection.

The Chair (Mr. Monte McNaughton): Mr. Clark, let's let Mr. Mantha finish.

Mr. Michael Mantha: He has a system, and I think our system that we have is similar. It's a tool that we utilize, which has proven to be quite successful.

We'd like to, in a way, legitimize that. If I'm hearing correctly from my friend Mr. Balkissoon, you'd want that process to be done through the Legislature. I just want to make sure that's—

Mr. Bas Balkissoon: No. I think what we, as a group, have to land on—if we all agree that members should have what you have, then we all have it and somebody has to pay for it, but it will reside in our constit office. Or

the simple method that I see as easy and workable and all the risk factors and everything else are gone and there's no privacy issue is the one most of the deputants who have come forward so far put in a neutral position, which is the Legislative Assembly has the database, server and the whole works, and it's managed by them; we as members get notified when there's a petition and here's the wording on the petition and there were 500 signatures on it.

1450

What we do with that is up to us. The Clerk will follow her normal process. When there is a petition and it's signed and it's legit, it goes to the responsible ministry, and they'll do exactly what they do today, it's just that it's now in electronic form and they can reply to everybody by email, if they put an email address on it.

We can also have a dual system. We can have that and we could still have what you have in your office. I think the big issue that it comes down to that we have to have a discussion on is the validation process you have on your website in your own riding. Is the assembly prepared to accept that? That's the part we have to discuss with the Clerk and the legal folks around here: Are we doing the right thing and is every possible protection and risk removed?

We could have a dual system. We could still have the paper system, because, to be honest with you, there are folks out there who will still want to write a paper petition and go door to door or go into a mall or whatever. We have to have a discussion at length on what it is we visualize this thing to be.

The Chair (Mr. Monte McNaughton): Mr. Clark?

Mr. Steve Clark: I just want to be clear as well that what I don't want is an expensive system when we don't require an expensive system.

Mr. Hillier and I used our websites—and I can use your websites as well, because you have e-petitions right now. Many of you do, Ms. Wong; a number of your MPPs—your government House leader has e-petitions on his. I'm just saying that many of our websites have the capability to do an e-petition now. What we have to decide is how easily do we want our constituents to be accessible for a petition. They have an expectation that they're going to get an answer.

I like some of the UK's model. I'm not particularly sure that the government will buy into the UK model of having a debate in the House if a petition gets a certain threshold. I get the sense that you probably wouldn't be too enthused about that. I think it would be great to have a debate about that because I think there are merits of having a more direct democratic opportunity when it comes to petitions. But make no mistake, people are still going to want to do that paper petition—some will. Some will prefer to deal with their MPP—because there are many constituents who want to deal with their MPP when it comes to a petition as opposed to dealing with some central website at the Legislative Assembly where I won't know whether they've signed the petition as my constituent or not.

I guess I had a sense, as a former House leader, that the government House leader had an interest in this and had an idea of where we should move forward. I just felt that we should add his voice, if he wanted to have his voice at the table, to where we move forward.

The Chair (Mr. Monte McNaughton): We're going to meet next week and continue.

Mr. Steve Clark: Hey, if the group wants to meet next week—listen, I've signed on to this committee. I know when it meets and I'm quite prepared to be here every week. But I do want something to happen.

The Chair (Mr. Monte McNaughton): I think it's pretty clear we're going to have a meeting next week to continue this discussion.

Are there any final, quick comments?

Mr. Bas Balkissoon: I just have a quick comment if you would allow me, because of Mr. Mantha's question of me.

The Chair (Mr. Monte McNaughton): Sure.

Mr. Bas Balkissoon: My only fear—and it was raised by several people—is what we received here as a committee from Mr. Hillier the first time—I got the impression he was the writer of the petition and people were signing it. To me, that's not a good process or a legitimate process. We are here to represent the people. We're not here to create petitions to create havoc. I put that out bluntly because that's my honest opinion.

The Chair (Mr. Monte McNaughton): Thanks, Mr. Balkissoon. Just a quick comment, Ms. Wong. We have to wrap up.

Ms. Soo Wong: The thing is, because of what the Clerk said to us, I still have questions. We were told at the subcommittee if there are any questions for the staff to do, that we should bring that forward. I think we should have that opportunity at the beginning of the meeting next Wednesday.

The Chair (Mr. Monte McNaughton): Okay. Sure.

Ms. Soo Wong: Because I still have not gathered, from all the witnesses today and the documents, the costs. I know the opposition says, "Let's find a cheap, easy way." The bottom line—

Mr. Steve Clark: No, not cheap and easy. I don't want an expensive process.

Ms. Soo Wong: I don't know. There will still be software costs. There are still the retention costs. There are still the archive costs. I don't know what it costs, okay? So, somebody get that information for me.

The Chair (Mr. Monte McNaughton): Okay. A lot of that, Ms. Wong, will depend on the system that we decide—

Ms. Soo Wong: Yes. We need the information on the system, then.

Interjections.

The Chair (Mr. Monte McNaughton): We have Trevor.

We'll see everyone next week at 1 o'clock.

The committee adjourned at 1456.

CONTENTS

Wednesday 21 October 2015

STANDING COMMITTEE ON THE LEGISLATIVE ASSEMBLY

Chair / Président
Mr. Monte McNaughton (Lambton–Kent–Middlesex PC)

Vice-Chair / Vice-Président
Mr. Jack MacLaren (Carleton–Mississippi Mills PC)

Mr. Granville Anderson (Durham L)
Mr. Bas Balkissoon (Scarborough–Rouge River L)
Mr. Chris Ballard (Newmarket–Aurora L)
Mr. Steve Clark (Leeds–Grenville PC)
Mr. Jack MacLaren (Carleton–Mississippi Mills PC)
Mr. Michael Mantha (Algoma–Manitoulin ND)
Ms. Eleanor McMahon (Burlington L)
Mr. Monte McNaughton (Lambton–Kent–Middlesex PC)
Ms. Soo Wong (Scarborough–Agincourt L)

Substitutions / Membres remplaçants
Mr. Grant Crack (Glengarry–Prescott–Russell L)

Clerk / Greffier
Mr. Trevor Day

Staff / Personnel
Ms. Joanne McNair, Table Research Clerk,
Table Research