ACCESSPRIVACY BY OSLER

AccessPrivacy Monthly Privacy Call – April 29, 2026

The lacking privacy framework for Canadian political parties: A roundtable discussion

Event details and recording link: available here

Moderator:
- Adam Kardash, AccessPrivacy National Lead, Co-Chair: Privacy and Data Management; Osler, Hoskin & Harcourt LLP

Speakers:
- Colin Bennett, Professor Emeritus, University of Victoria; Associate Fellow, Center for Global Studies
- Michael Geist, Canada Research Chair in Internet and E-Commerce Law, University of Ottawa

Webinar Transcript*

Adam Kardash (00:01):
Hello everyone, and welcome to the Access Privacy Monthly call.

Recent amendments to the Canada Elections Act have resurfaced an issue we visited before on a previous Access Privacy Monthly call, and that is the absence of a robust framework governing personal information in the custody and control of political parties.

The context for this issue is quite striking. The Liberal government is expected to introduce legislation to replace PIPEDA in the coming months. The new framework, which will be similar to Bill C-27 containing the Consumer Privacy Protection Act—which died on the order paper in January 2025—is expected to establish a comprehensive statutory suite of obligations for private sector organizations backed by meaningful enforcement. Call attendees may already be aware that the federal government has also launched a consultation to support modernization of the Public Sector Privacy Act, engaging interdisciplinary experts on a range of themes and policy approaches for that reform effort.

Both of these reform efforts—private sector and public sector privacy—are anchored in a core policy objective, which is in essence strengthening trust in the Canadian data ecosystem. This makes the political party gap in privacy protection all the more conspicuous. The absence of a rigorous privacy framework for political parties and the

*Generated by AI

parties' continued resistance to one has produced one of the rare moments in the Canadian privacy arena where there is a near consensus across academia, civil society, privacy regulatory authorities, and private sector stakeholders that the status quo with respect to the protection of personal information of Canadians in the control and custody of political parties right now is untenable.

To illustrate this gap, we've prepared a snapshot comparison of PIPEDA's requirements for private sector organizations against the privacy obligations imposed on federal political parties under the Canada Elections Act as amended. Colleen, if you could just put it up on the screen—you'll see that we have this table where it contemplates both the suite of requirements that we'll go through quickly, the PIPEDA articulation of whether that requirement exists in PIPEDA, and then an articulation, a snapshot summary of whether that corresponding requirement exists under the Canada Elections Act, including as further amended by Bill C-25, which is currently at second reading.

If you just scroll down, Colleen, a bit—under PIPEDA, there's enforcement by the Office of the Privacy Commissioner of Canada. This does not exist under the Canada Elections Act. The Canada Elections Act does require organizations to designate an individual, its chief privacy officer, and that's corresponding to PIPEDA's requirement. But notably, the requirement is for the privacy officer to oversee the party's compliance with its own privacy policy. It's an awkward way of framing the overall obligation—not with statutory requirements generally.

PIPEDA, and the pending reform under private sector privacy law, has privacy management program requirements. There is no requirement under the Canada Elections Act for political parties to document and implement policies and practices to ensure compliance with statutory requirements. There is a requirement under the Canada Elections Act to have privacy policies and post them. As amended, this would include the name and contact of the CPO for the political party, the type of personal information that would be collected, how it would be used, a reference to the nature of training, and a violation of the statements in the privacy policy would lead to a contravention subject to AMPs—but those AMPs are $100,000 max, which pales in comparison to the enforcement regime, at least as proposed under the CPPA.

Notably, there is no requirement to obtain consent for the collection, use, and disclosure of personal information. PIPEDA, and the reform of PIPEDA under the CPPA, contains a powerful overriding obligation—currently under Section 5(3)—that organizations are only able to collect, use, or disclose personal information for purposes that a reasonable person would consider appropriate. This is absent from the Canada Elections Act.

If you scroll down a bit, there are, however, some statutory prohibitions that are enumerated in the Canada Elections Act, which were introduced in Bill C-25, but these are narrow. One is a prohibition on providing false or misleading information about, in

essence, what would be set out in the privacy policy. There's a prohibition on selling personal information—notably, the term "selling" is not defined. It has a lot of meaning if you look to statutory regimes in California and otherwise, so it's at minimum vague.

Then there's a rather odd prohibition that disclosure of personal information to the public for the purposes of causing harm is prohibited. So a pretty narrow set of prohibitions, certainly much narrower than what would be caught by the concepts and the principles set out in Section 5(3) of PIPEDA.

There is no requirement under the Canada Elections Act, even as proposed under C-25, for retention of information only as long as necessary to fulfill identified purposes. The interesting thing about this is that Section 446.2 of the Canada Elections Act contemplates—and this is the quote—"a national, uniform, exclusive and complete regime applicable to registered parties." And then it includes requirements relating to collection, use, disclosure, retention, and disposal. So you have this odd context where there's a purpose clause that is not, or does not appear to be, operationalized within the statutory wording within the text.

There's a requirement under PIPEDA, of course, for safeguarding. This is present in the Canada Elections Act, although it's oddly articulated as a requirement to include that statement in your privacy policy. So in effect, it's a requirement stated rather oddly.

There is no requirement to retain records of any breach of security safeguards. There is no requirement under the Canada Elections Act to report breaches to the Office of the Privacy Commissioner of Canada. There is a requirement as proposed under C-25 that the privacy policy require the party to take appropriate steps, including informing affected individuals. So in effect, there is a notice requirement when there is a real risk of significant harm and an incident gives rise to that.

But if you go to the next page—and it really is the kicker to this comparative table—individuals and the public will not have a statutory right to access their personal information. This doesn't exist under the Canada Elections Act. There's no right of individuals to correct inaccurate or incomplete records held by the political parties, and there's no data portability right. PIPEDA just got amended, as call attendees may know, to include a data portability right, which would apply to entities that are set out in a data mobility framework. Nothing of that at all is set forth in the Canada Elections Act.

So this comparison chart was meant to provide context for today's discussion. You can take it off the screen. What we want to do with that context is turn now to the discussion and just dive right in to explore this issue further.

Today I'm joined in this conversation by two returning guests to our call. Very thrilled to have both of them. First, Colin Bennett, who's Professor Emeritus at the University of Victoria and an associate fellow at the Centre for Global Studies, and really one of Canada's foremost scholars of political party privacy and surveillance concepts. And Michael Geist, who is currently the Canada Research Chair in Internet and E-commerce Law at the University of Ottawa, and also a leading voice in Canada, specifically on Canadian digital policy and legislative reform. Colin, Michael, thank you to both of you.

Michael, I'm going to turn to you first to help level set here. What are we really actually talking about? What is the nature, sensitivity, and volume of personal information that is held by federal political parties, and how is it being used?

Michael Geist (10:13):

Thanks for that, Adam, and thanks for having me back on what's become such an important source and a place for discussion around privacy-related issues. So when we're talking about this issue—and you've done a really nice job of outlining how the legislation for the private sector and political parties differs—we're talking about entities that hold information that would largely rival, I think, at least mid-size private sector firms, if not more. We're talking about a significant amount of data.

It typically starts with privileged access to data that no other organization gets. The Canada Elections Act allows the parties to get a list of the electors from Elections Canada. And so that's like a base layer—name, address, unique electoral ID for every voter and every riding. But once on top of that base layer, the parties themselves have a voter relationship management system, essentially the political version of a CRM.

Each of the parties has their own version and it builds in a ton of data. We're talking about, as I mentioned, some of the statutory data that includes the electoral list. But beyond that, there might be information that's collected directly by the parties themselves. This includes notes when they're out canvassing, requests that might come in for signs on someone's lawn, donation records, whether they show up at various events, signatures on petitions, and things like that. Do they open emails? What are their click rates? Perhaps that kind of stuff.

Then there may be a further overlay on the commercial side—third-party information around social media analytics and information they might get from data brokers. So a pretty broad range of additional stuff. And then on top of all of that, there's essentially data that is either derived or inferred from different kinds of activities that they're engaged in.

They'll develop a support score—how much can you count on this person? What are their core issues? What is their likelihood of donating or volunteering? What can the

parties infer when it comes to someone's religion or ethnicity or age? There's just a whole range of different things that they're capturing.

They use this for a really wide range of different things. It's for get-out-the-vote type activities. It's for micro-targeting that might occur online—say, in social media or otherwise for some of the advertising. It's for donor activities to try to get people to donate to the various parties. It might even be used to vet candidates or engage in opposition research.

I should note, just on a very personal level, I experienced this actually a number of years ago firsthand, where I had met with the then-MP for my riding, who was a cabinet minister—it was John Baird at the federal level. We'd met, I guess, about a year or two before this incident took place. I think we were talking about copyright and some digital policy-related issues.

A couple of years later, I'm driving in my neighbourhood in Ottawa and there's a pack of several people who are doing door-to-door canvassing, actually not for the federal level, but for the provincial party. Baird is there alongside the local candidate at the time. And Baird is one of these politicians who has this incredible memory for people's names and faces. I'm just in a minivan and I pull up, and Baird sees me. He's like, "Hi, Michael. It's nice to see you," kind of thing. I was amazed that he knew who I was, and he introduces me to the candidate.

In the aftermath of that, living on that street, I started getting regular cards from the parties, including cards around Jewish holidays—I'm Jewish. My mezuzah might well have been on my door. So someone would infer that I'm Jewish coming out of that. On election day, I got multiple phone calls from that candidate on the assumption that I was a supporter of the party.

What had happened, of course, was that all of these bits of data were collected, added into the database, and then used for exactly these kinds of purposes. All the parties do it. And as I'm sure we'll talk about, all the parties would like to have as few guardrails around using that data as possible.

Adam Kardash (14:35):

Michael, your description of your personal experience resonates with me. This issue was triggered for me when I received a card in advance of the Jewish High Holidays. And I remember saying to myself, "Oh, it's very nice," and immediately thinking, "How is it possible that I'm getting a card from a political party relating to my religion?" It ended up having me think quite deeply about this particular issue. Colin, can you share more information about the nature of the personal information holdings of political parties?

Colin Bennett (15:16):

Thank you, Adam, for the intro. Just to add to what Michael was saying, these voter relationship management systems are now over 20 years old. They were first begun by the Conservatives, and then the Liberals developed them in consultation with US consultants—that's another important dynamic here. The Canadian political parties learned a lot, particularly from the Obama campaign, about how to develop these systems and build them and use them for targeting across a variety of different methods.

You asked what we know about what's in these systems, and the honest answer is that we don't know as much as we should because they're shrouded in secrecy. Because they're not subject to our privacy laws, it's not really possible to officially access them. The privacy commissioners generally don't have any ability to investigate, with one exception—and that's in BC, where our Personal Information Protection Act does apply to provincial political parties and has done for 20 years.

There's a question about whether it also applies to the federal political parties, and we'll get onto that. But the BC Commissioner did an investigation back in 2019 into provincial political parties, and it's really the only official record that we have about what's in these systems.

Just to build on what Michael was saying, here's some of the information that they found: sex, ethnicity, age, language, religion, income, education, family marital status, profession, workplace name, job title, profession status, number of years at residential address, demographics, issues of interest to the individual, and then a whole range of different IDs such as LinkedIn ID, Skype ID, Facebook ID, Twitter ID—and it goes on. And that's on top of the public party participation data that they know about: have you voted, will you vote, and so on. It's extensive.

You can only infer that if that was the kind of data that was collected by BC's poorly resourced provincial political parties in 2019, far more is captured by the federal political parties today. So it's a complex picture, but it's also a picture that's shrouded in a lot of secrecy, and that's a situation that shouldn't be allowed to continue.

Adam Kardash (17:57):

So what we have here is a very large and growing amount of very sensitive personal information of Canadians within the custody of each of the parties-

Colin Bennett (18:12):

Sorry, Adam, just one further point on that. The other big question here is how that information is then used to profile individuals for social media outreach on Facebook or Instagram and so on and so forth. That process is also shrouded in a certain amount of

secrecy because they use that in order to develop the profiles to micro-target citizens across a whole range of different issues.

Adam Kardash (18:39):

That's right. That's an excellent way of framing it—that there's a diverse range, a high volume of sensitive information compounded with derived data, inferred data, all of which creates quite a sensitive picture of the individuals to whom it relates. Colin, share with us the legislative and regulatory history of the privacy protection of political parties—or really, frankly, the lack thereof. Can you share for a few minutes just to level set for everyone?

Colin Bennett (19:18):

I did a report for the Privacy Commissioner on this issue back in 2012. This was from Jennifer Stoddart, because she was receiving complaints about members of parliament and political parties, and she felt she couldn't do anything about it. So she asked me to do a little report, which then inspired my interest in the subject.

We know that PIPEDA doesn't apply to federal political parties because the former Privacy Commissioner, Daniel Therrien, said so. That was in response to a complaint that was lodged by the Centre for Digital Rights, which says basically that what political parties are doing is commercial in nature. It is a sort of quasi-commercial activity. After all, they build databases, they do a lot of marketing, they engage in social media outreach, and really it's a marketing strategy—therefore PIPEDA should apply. Daniel Therrien said, no, it's not.

So we know that. They've exempted themselves successfully, generally speaking, from legislation such as CASL, the anti-spam legislation. There are some rules about telecommunications, the telemarketing rules that are administered by the CRTC—some of those rules apply to political parties, but not the same as apply to commercial organizations. So you're left with the rules that are in the Canada Elections Act.

One further point about this: a few years ago, we put in a complaint to the Commissioner of Elections saying that the voters lists that are legally shared with political parties have to be used for the "purpose of communicating with electors." And there hasn't yet been any legal clarity about what that word means. So the argument was that building databases and profiling citizens is over and above that requirement. We also know that these databases are used for purposes other than communicating with electors, such as checking on judicial appointments.

So there were some reasons there to ask the Commissioner of Elections to investigate this to determine whether or not the data that's shared and used to build these massive databases is in fact solely used for the purpose of communicating with electors. And

after a lot of to and fro the commissioner said, "No, we're not going to investigate that." And the court agreed with them.

So basically we're down to what's in the Canada Elections Act, as you have described, and what is in certain provincial laws, primarily BC's Personal Information Protection Act. There are also some rules in Quebec's new Law 25, which apply to provincial political parties. So that's basically the overview.

Adam Kardash (22:31):

Michael, there's been such resistance over the years by the political parties. Before we delve into some of the aspects of that, I think it would be really helpful for you to set out what's the stated rationale. What do the political parties state as the reason why they're resisting a statutory regime that has much more alignment with private sector privacy laws federally?

Michael Geist (23:04):

Well, I must admit, I'm inclined to be flip and just say naked self-interest. But at times there is a willingness to go beyond that, though frankly, none of the arguments would really, I think, be viewed by many as particularly credible. So note that these are not what I'm trying to make the case for—this is what they try to make the case for. I'll highlight at least a few things.

First, they oftentimes argue around democratic participation. This notion that political parties are core to democratic participation, and the argument would be that if they don't have the ability to collect and use this information in this way, it's going to impair their ability to communicate with voters. Of course, that's true for every organization that collects information—they want to engage with the people whose information they're collecting.

Privacy law fundamentally requires certain kinds of standards in order to be able to do that, like consent and purpose limitation. And accountability—of course, they just don't want to face that. They often argue a freedom of expression argument, which I must say I find to be both a disingenuous argument—this notion that somehow this speech is free speech that is beyond the realm of being regulated—but it's also a dangerous one, especially for those that believe in privacy legislation broadly applied in Canada. The same kinds of arguments could be raised in other contexts, and so I think there are some real risks there. But I don't think it's a particularly strong one. We see these kinds of limitations in other contexts, and there isn't really a prohibition or even a limitation on their ability to express themselves—merely potentially some limitations or at least guardrails around what they do with people's information.

Or they argue what might be defined as an operational necessity argument. They say, "Listen, we need the data to run these kinds of campaigns." But of course, there are lots

of organizations that need data for various kinds of things—that doesn't absolve them of the need to meet standards. It simply suggests that there's a lot of value there, and that helps explain why people would comply with various rules.

Fundamentally, at the end of the day, I think they run these up the flagpole, but I don't know that anybody thinks that they're particularly credible. I was speaking to one senator who heard some of these arguments in the context of Bill C-4 and the parties' efforts, and the response I got from the senator was that if anything, it made the senators more inclined to want to regulate. They just didn't find these particularly credible.

Because at the end of the day, what is really happening is, as Colin mentioned, this goes back a couple of decades. You're dealing with a 20-year infrastructure of data practices that had limited or no real external accountability. To bring in these kinds of rules would require presumably some amount of retrofitting on consent, developing some limitations on how the data can be used, access rights, correction rights, independent oversight—the very things that I suspect most people on this call are accustomed to and are actively part of their day jobs in terms of ensuring that their organizations are compliant.

So the resistance here, I don't think is principled—it's operational. They want to continue to operate in the way they always have. There are real costs that would be imposed if there were these kinds of changes. And so that helps explain why there is such widespread opposition. As has been noted, all the parties do this, and so all the parties are by and large of like mind when it comes to this, because they'll all be affected in much the same way.

Adam Kardash (26:49):

Just before we turn to the current state of play, Colin—you and I spoke at the last monthly call about this topic—about, number one, there really being no compelling public policy rationale, exactly as articulated by Michael. And notably, there are regimes, including Europe, where political parties are subject to privacy laws and don't appear to be materially impacted. Can you just share some of those comments? Because I think that's so important to hear that perspective.

Colin Bennett (27:23):

Just to add to what Michael was saying about the resistance, another couple of arguments you get is that this would encourage vexatious access to personal information requests during a campaign—that one party will then use this law in order to impede the procedures of the other party. Well, that has never happened that I know in any other country where this has occurred.

The other thing you get is, “Well, we rely on volunteers, and that’s important. That’s been part of the democratic mobilization process to have all these volunteers going around the doors and so on. And if the rules were too tough and if the sanctions were too tough, then we wouldn’t get volunteers.” Well, that too is also not borne out by overseas practice.

The vast majority of democracies in the world—principally those that are covered by the GDPR or GDPR-like legislation—political parties are covered by privacy legislation, comprehensive privacy legislation. There are amendments, there are changes, there are tweaks to the law in order to facilitate the communication to electors. There are changes that have been made which recognize that political parties are not the same as commercial organizations.

In addition to that, data protection agencies in the UK, in Ireland, in some European countries, have issued reports on political parties, and they’ve engaged with the political parties, given them recommendations—as they do with government and with commercial organizations—about how best to improve their practices. And to a large extent, this is not a conflictual process. The parties there have engaged with the commissioners in good faith and they’ve used the expertise of the commissioners in order to improve their practices.

So this really shouldn’t be a threat. We tend to see that the federal political parties in this country have circled the wagons—they see the outside forces as a threat. I don't feel that there are many people within the political parties that are really seriously informed about these issues and who attend privacy conferences. I don't know whether any of them are going to be listening to this call, but my engagement with the people in the political parties is that they need some education on these questions. And that education will perhaps make them see that this is not a threat, and they can perfectly well perform their role in Canadian democracy and at the same time comply with contemporary privacy standards.

Because after all, we are talking about democratic issues here. We’re not just talking about commercial marketing—we’re talking about databases and practices that affect the health and resilience of our democracy. It’s more important, in my judgment.

Adam Kardash (30:35):

You’ve both alluded to this already, but Colin, today, where do we stand now legally and politically? We’ll turn to advocacy in a moment, but legally and politically, where are we today?

Colin Bennett (30:47):

Well, the complaints to the BC Privacy Commissioner—which occurred by BC citizens over four years ago—were adjudicated by the commissioner, who said that the BC law does apply to federal political parties to the extent that they're active in BC. That decision was upheld by the BC Supreme Court, with the judge using some very strong language about the importance of this issue for the health of our democracy. The political parties have unanimously appealed that decision, and it's going to be heard, we understand, by the Court of Appeal at the end of May.

Of course, once you get into these questions, they get mired in complex constitutional questions concerning federalism and whether or not the Canada Elections Act should be paramount over whatever a province should do. But the argument is that really what BC has done—or indeed what Quebec has done, should it choose to go this far—doesn't really interfere with what the Canada Elections Act has said. It just goes the extra mile. And if the political parties have got to do a little bit extra in BC and/or Quebec, then so be it. That's the nature of Canadian federalism.

But that's all going to be argued out in the Court of Appeal. And one assumes presumably to the Supreme Court of Canada further down the road. So that's where we are.

Adam Kardash (32:26):

And the principles of Marcotte, Supreme Court of Canada, and Molson would align with what you just set forth, Colin. Michael, any additional comments on where we are today legally and politically?

Michael Geist (32:38):

Yeah, I guess we didn't really talk so much about that whole political process that C-4 underwent. And it's probably worth highlighting because it does give, I think, a really strong sense of the political side of what we've seen play out here.

We need to go back just a little less than a year ago when we had a new government and concerns about the US administration, Donald Trump, and the sense that the government wanted to act very quickly. It introduced a series of bills very fast, including C-2, which included—buried at the very end—lawful access legislation. The government has had a restart on that after it clearly overshot and raised some real concerns from a privacy perspective.

And then it also had this C-4, which was nominally an affordability measures bill with a series of tax-related reforms. Buried at the very end were these changes to political party privacy, which were not only weak—they were even weaker than some of the prior proposals that we had seen earlier.

The government did its utmost to ensure that there was no discussion about it. It was as if it was almost Kreskin-like—going to somehow make all of this magically disappear and nobody would think about it and nobody would talk about it. So it wasn't talked about during the House debates. And once it went to committee, the committee did its very best to act as if this didn't exist at all. In fact, despite requests, they refused to hear from any witnesses that wanted to speak out on the issue. I think someone calculated that it was about 30 seconds total during the committee hearings where the existence of all these provisions was just acknowledged.

So the government does its best to ensure that nobody's paying any attention or it's not discussed. It ultimately goes to the Senate. And at the Senate hearings, the senators—who are somewhat less politically aligned, many of them are still politically aligned but not in quite the same way, certainly not beholden to the political parties in quite the same way—actually do conduct a hearing.

I think it's fair to say that many of the senators are pretty appalled by what they've seen. They can see exactly what we've just been discussing. They can see what is really at play here. They're clearly left extremely uncomfortable with simply rubber-stamping this through. There are a number of proposals put forward, everything from just jettisoning out of this Bill C-4 the political privacy provisions altogether.

But there are many senators that say, "Listen, we're not elected. There's a limit to what we ought to be doing, especially in the context of a bill that is primarily about tax-related measures." And so they come back with a solution where they say, "We're going to create a sunset clause for this. We're going to say that you've got three years to come up with real privacy. And if you don't, what you just created here will come to an end and we'll go back to the previous situation." And they send it back to the House, which itself is a pretty strong step. You don't see the Senate do that all that often.

And the House simply rejects it. They say, "Thanks, but no thanks. That's not what we're going to do." And it gets kicked back to the Senate, and all in the span of less than a day—or at least one legislative day—we get the House saying, "No, we're not going to take on board your proposed reform." It goes back to the Senate. The Senate says, "Okay, we tried." And they give it a rubber stamp and say, "Okay, fine. We will pass it as is." And it receives Royal Assent a couple of hours later.

So there was some effort to raise concerns associated with this, but at the end of the day, it got steamrolled.

We now have, as we've been mentioning, C-25, which is an effort to at least put a little bit more meat on the bones of privacy. But I think most who take a close look at it say we are still nowhere near the kinds of standards that we would typically expect of any

other organization, much less organizations that have data with the kind of sensitivity that we've been talking about.

Adam Kardash (36:32):

And Michael, comments on current advocacy efforts?

Michael Geist (36:37):

There have been real efforts, and people like Colin are some of the people that really lead the way. I think we can think of it in a number of different places. We should note that privacy commissioners have, of course, been very consistent on this issue. So you don't have to take an academic's word for it. You can take a look quite clearly and see that the Privacy Commissioner's consensus position over now a number of commissioners has been that these are real issues and there are real problems with these rules as the parties themselves are proposing, and that's a problem.

At the parliamentary committee level, we have seen the ethics committee look at this issue in the past. Once MPs or politicians are able to remove a little bit their political hat and think at least somewhat independently, this whole thing feels like a bit of a no-brainer. And so we get recommendations to do things along these lines that would move us closer to the standards that the private sector faces. It's once the parties themselves and the government itself comes in—and as I say, all the parties are by and large of like mind here.

What has been interesting, and Colin may want to talk a bit more about this, is some of the effort that we see on the civil society and academic advocacy side. There are people like Colin, Sarah Bannerman, and others that have been very active consistently in citing these issues and trying to raise public awareness. And then, of course, we've got the litigation that we've made reference to. That BC litigation is in many respects a form of advocacy. It was done by and large to seek to try to influence not just the rules that would apply to people in British Columbia, but essentially to try to move this issue forward on a national basis and try to see some kind of real change.

So despite the efforts, I think, of the parties themselves to kind of wish this away, the reality is there's been an ongoing concerted effort from many in the privacy community, ranging from the commissioners all the way on the spectrum to many in the academic world and advocacy world. You've got a number of different groups that have been active—BC FIPA in particular has been really active on these issues. And I think they have succeeded in at least keeping the spotlight on it and unveiling or ensuring that we've got the kind of litigation track that Colin mentioned a moment ago.

Adam Kardash (39:12):

Colin, can you provide a little background on the nature of the activities you've been involved with and others, and where they stand right now?

Colin Bennett (39:21):

Yeah, I mean, I've been banging on about this for 12, 13 years or more. And then the Cambridge Analytica scandal hit the headlines and then things progressed from there. But if you look at what has been done, it's difficult to know what else could be done.

There's been a lot of press. Several journalists have been informed about this and kept informed. The civil society organizations have been mobilized—that's Open Media, BC FIPA, the Canadian Civil Liberties Association, as well as the Centre for Digital Rights. There's been parliamentary hearings, there's been litigation, there's been academic research done by myself and a number of others as well, it has to be said, in both Quebec and English Canada. So it's difficult to know what else could be done.

There's a campaign underway right now mobilized by those organizations. There are public opinion polls—one's out which says, interestingly, that only around 30% of Canadians trust political parties to protect their personal information. And if this issue's about trust, then those parties need to be looking at that very, very carefully.

But you are confronted with this unfortunate reality that you are up against not commercial interest, not moneyed interest—you're up against political power, and you're asking political parties to surrender control over a resource, namely personal data, which has to some extent and to an increasing extent got them into power. This attitude is pervasive amongst our political parties and the consultants and the organizations that work for them.

And so therefore you have this sort of race to the bottom that's very, very difficult to reverse because you have to say, "Look, we need a level playing field here. We need clarity, we need transparency, we need some rules." But you're asking the political parties in power to basically surrender the resource that got them there. So that's a very different character of political battle, in my judgment.

So we'll see what happens. The parties want this litigation to go away. They're spending enormous amounts of money on this, and that's not in their interest or anybody else's. So the pressure will be kept on, on all of those fronts, and we'll see what transpires.

Adam Kardash (42:04):

As I mentioned at the outset of the call, this is a topic that is of interest to many stakeholders that we interact with. We're going to continue to monitor the advocacy efforts closely to see what, if any, material developments will happen to enhance the privacy protections in this particular context.

I just want to thank you both, Michael and Colin, for your time. Very, very interesting, insightful. And I know on behalf of call attendees that it'll be very much appreciated. And

most of all, I'd like to thank everyone who's joined the call. We appreciate it, and we look forward to having you participate in the next monthly call. Thank you very much.

* * *

*Generated by AI