OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

CHECK AGAINST DELIVERY

SPEECH TO THE
SPECIAL COMMITTEE TO REVIEW THE PERSONAL INFORMATION PROTECTION ACT

February 23, 2021

Michael McEvoy
Information and Privacy Commissioner for British Columbia

Good afternoon, Chair and members of the Committee. It is important to me to respectfully acknowledge that I present to you today on the traditional territories of the Lək̓ʷəŋiṅəŋ people, known also as the Songhees and Esquimalt First Nations.

With me today are Deputy Commissioners Jeannette Van Den Bulk and oline Twiss, and Senior Communications Manager Michelle Mitchell.

It is again my honour to appear before you, to provide an update on a very important development since our last meeting in September. As you have learned, the federal government recently introduced Bill C-11 that proposes new federal privacy legislation. The essence of it is that the Consumer Privacy Protection Act (which I will refer to as the CPPA) will replace the *Personal Information Protection and Electronic Documents Act*.

This development has a significant bearing on your deliberations and, as I will explain, adds greater urgency to reform of British Columbia's privacy legislation.

This afternoon I will focus on key provisions of the CPPA that impact British Columbia's *Personal Information Protection Act*. I will do that in the context of recommendations I made to you last September; recommendations, I would add, that are even more relevant today.

I am also going to address questions, I understand from the Committee clerk you have, about Europe's *General Data Protection Regulation*, the GDPR, and its relation to PIPA reform.

When I last spoke to the Special Committee, I observed that PIPA, drafted nearly two decades ago, requires urgent reform to meaningfully address the growth in digital economic activity and the challenges posed by new technologies. Artificial intelligence, data analytics, facial recognition, and social media are just some of those challenges. The federal government launched its legislative response to these issues late last year with the introduction of the CPPA. All eyes now turn to BC's government to see whether it will meet this moment.

What I also emphasized in our last meeting was the need for PIPA, our law, to be harmonized, to the greatest extent possible, with laws developing nationally, and internationally. As my supplementary submission explains, enactment of the CPPA will leave PIPA's status up in the air unless it is declared substantially similar to the CPPA. This greatly underscores the need to act now to update PIPA.

To be clear, I am not advocating for a simple copy and paste of the proposed federal legislation. There are a number of provisions in the CPPA that are not fundamental to substantial similarity and do not further the privacy rights of British Columbians and therefore should be left out of BC's PIPA.

This Special Committee has the unique opportunity to recommend refinement of the positive aspects of the CPPA to suit the needs of British Columbia, while maintaining harmonization and leading-edge legislation.

When PIPA was first introduced in 2003, the then minister responsible observed that, and I quote, by "retaining provincial jurisdiction over this important aspect of provincial commercial activity, [PIPA] will reduce the regulatory burden for the BC private sector, fill in significant gaps left by the federal act and provide provincial oversight instead of oversight by a federal commissioner located in Ottawa."

Chair and Special Committee members, these observations remain true. PIPA was, in part, a response to the then newly minted federal government's PIPEDA, the *Personal Information Protection and Electronic Documents* Act. British Columbia's policy makers set out to fashion a law that reflected the province's needs while enabling BC's enterprises to do business domestically and internationally. They also sought to create a law that enables individuals to trust that their privacy is appropriately protected. These policy imperatives, I would respectfully submit to you, should remain central in your deliberations.

I have mentioned international developments and the need for our laws to keep pace with them. I canvass this more fully in my supplementary submission, but it is sufficient to say here that the CPPA, Ottawa's legislation, is to a significant degree a response to international developments; specifically, the European Union's GDPR. The GDPR's enactment in 2018 was an absolute game-changer internationally. It dramatically raised privacy standards and its reverberations have been felt well beyond Europe's borders. Companies, including those in Canada expecting to do business in Europe or with European companies where personal information is involved, are required to meet GDPR standards.

The need to meet European standards is not new. This was the case under the GDPR's predecessor, the data protection directive. That directive greatly influenced Canada's original decision to enact PIPEDA and how that law was framed. In the result, Canada received adequacy status – very important because it allowed the free flow of personal data between businesses in Canada and the European Union. Maintaining adequacy is crucial to Canadian and European trade. It would be astonishing to believe that the CPPA's recent introduction was not in large measure prompted by the GDPR and a desire to ensure Canada's new law is seen to be adequate in the eyes of the European Commission.

You may be sensing something of a domino effect going on here. Europe sets off change in Canada's federal privacy law, which in turn sets in motion an imperative to amend BC's privacy law.

Why? Because federal law requires provincial privacy law to be substantially similar in order to be valid.

It is quite clear that, in light of the GDPR and the proposed CPPA, British Columbia is now obligated to step up to the plate. Will we seek to reform PIPA so that it is substantially similar to the CPPA and in effect aligned with the global benchmark GDPR?

The dynamic here is one in which jurisdictions try to move in step, harmoniously, though not identically. Being at the tail end of this process, as we are, has certain advantages. You as legislators and our policy makers can adopt the best of breed in what is found elsewhere that is both suited to British Columbia and harmonious with other laws.

I want to now turn to the proposed CPPA in more detail.

The CPPA will be enacted by the Digital Charter Implementation Act, 2020. It is part of the federal government's Digital Charter initiative which began some five years ago. The recent legislation is referred to in shorthand as Bill C-11, which is the Bill the government tabled last November.

Before tabling Bill C-11, the federal government conducted consultations on privacy laws and the digital economy. In 2019, the government released a report on those consultations. The report concluded that, and I quote, "the current privacy legislation, PIPEDA, needs to be modernized and streamlined. However, the Government must ensure that updates both support innovation and protect Canadians. Rules must be supported by clear guidance on implementation and applicability and must consider effective and appropriate enforcement measures to hold players accountable and ensure Canadians have confidence and trust in these protections."

The CPPA will retain some features of PIPEDA while significantly strengthening protections for individuals and ensuring that those rules remain balanced and are not a barrier to economic activity. What do the proposed new federal rules mean for modernization of PIPA, our own almost 20-year-old privacy law? What do the proposals mean for the recommendations I provided you last autumn?

When compared to the CPPA's key features, our earlier recommendations to you illustrate how there is a core consensus on what is needed to update Canada's private sector privacy laws. Fully 10 of my 12 recommendations to the Committee last fall are found in some measure in the CPPA. The detailed written submission I have provided you addresses each of these 10 recommendations in relation to the CPPA proposals. Today, I will simply highlight some of the key ones, describing how they align with – or in some cases differ somewhat from – the CPPA. I will explain how BC can implement the CPPA's core concepts while improving upon Bill C-11.

I begin with what is one of the most important changes the Committee could recommend – mandatory breach notification.

The CPPA will essentially replicate PIPEDA's existing breach notification requirements. This aligns completely with the previous recommendations I have made to you on this issue.

I will stress once again the importance of harmonizing PIPA's breach notification rules with the CPPA, and with comparable Canadian laws, including Alberta's *Personal Information Protection Act*, which has had breach notification rules for over a decade.

To recap, I am recommending that PIPA should require organizations to notify both affected individuals and my office of privacy breaches that meet a threshold of risk of harm to affected individuals. PIPA should also authorize my office to require an organization to give notice to affected individuals if the organization has failed to do so, including where we learn of the breach from a source other than the affected organization.

How important is this breach notification fix for PIPA? PIPA is far behind comparable Canadian privacy laws, but it is also behind internationally. The EU, the UK and all 50 US states—yes, all 50

states—now have some form of mandatory breach notification law. Further, reforming PIPA on this issue is, in my view, likely to be of considerable importance in the federal government's assessment of whether PIPA is substantially similar to the CPPA.

The second matter I want to highlight today is something I spoke about in detail in my September submission to the Committee, namely, the right of individuals to consent to the collection, use and disclosure of their personal information. The overarching aim of modern privacy laws is to give individuals appropriate control over their own personal information, and consent is at the heart of that concept. As other laws do, PIPA ensures that individual privacy rights are at the forefront by requiring organizations to obtain consent unless an exception applies.

One of the challenges of PIPA is its now-inadequate bilateral approach to consent—the assumption that there is a straightforward, simple transaction between one business and one customer. We all know that, while there are situations where this works, it is an increasingly unrealistic assumption in our modern digital age.

This challenge is not unique to BC, and it is something policy makers have grappled with for years. Under the heading of my third recommendation to the Committee last autumn, I made three specific recommendations for an improved approach to consent, to better protect individuals without imposing undue burdens on businesses.

Those recommendations require an organization to put in writing the purposes for the collection, use and disclosure of an individual's personal information, unless there is a good reason to allow the organization to rely on implied consent. They also stress that it is important for an organization to use plain language in describing these purposes. And finally, when it comes to privacy, such written notices must stand out on their own and not be wrapped in dozens of pages of legalese.

The CPPA also proposes to update the consent requirements found in PIPEDA. However, as you will read in my written submission, I have serious, very serious, reservations about elements of the proposed CPPA consent provisions. Specifically, the CPPA would introduce new exceptions to consent that are very broad, or ambiguous, and would reduce, even eliminate, transparency for individuals.

To offer only one example, the CPPA would enable organizations to, in some cases, secretly collect, use, and disclose our personal information without having to tell us what they are up to. This is inconsistent with long-accepted, internationally recognized data protection principles. I am not alone in expressing these concerns and it will be interesting to see what this might mean for the CPPA's and Canada's adequacy when measured against the GDPR.

I urge the Committee to reject the proposed CPPA consent exceptions as a model for PIPA. To be

clear, exceptions to consent are appropriate—and PIPA already has consent exceptions—but modern privacy laws remain consent-based by default and exceptions should be limited, narrow, and clearly justified.

What I would urge the Committee to affirm that the concept of an individual's control over their own personal information is, through consent, a core principle of PIPA.

I'd like to move on to another key recommendation from my previous submission, recommendation 4, which concerns automated decision-making.

Information technologies are evolving in ways, and at rates, that can raise serious risks for individual rights and interests. Advances in data analytics and artificial intelligence can undoubtedly help improve services to individuals and communities. However, they can also create serious risks for privacy rights.

Consider the example of an individual who fails to screen in for a job opportunity based on the decision of a machine. The information used in that process may be outdated, false, incomplete, or otherwise defective, yet the outcome has a significant impact on that individual. The algorithm used to make the decision may have built-in, if unconscious, biases—a fault already discovered in decision-making algorithms. Critically, under the proposed CPPA, there is no obligation on the organization's part to accompany the decision with an explanation that it was made by a machine. and thus, no opportunity to know about it let alone challenge it.

The GDPR by contrast contains significant protections for individuals by giving them the right, with some exceptions, to prohibit an organization from making decisions about them based solely on automated processing of personal information. And amendments pending for Quebec's privacy law also provide some protection in this area.

Without mincing words, the proposed CPPA falls short of what I believe is necessary to protect citizens from the use of opaque, otherwise unregulated automated decision-making technologies. The CPPA would merely require an organization to provide a "general account" of its "use of any automated decision system to make predictions, recommendations or decisions about individuals". The CPPA says that this general account should be written into an organization's policies and procedures. What does this mean practically? It almost certainly means the description of the general nature of an organization's automated decision making will be buried in lengthy legalese along with many other matters.

In light of this, I reaffirm my initial recommendations to the Special Committee last fall, which would require an organization using automated processing of personal information to offer specific transparency disclosure, disclose the reasons and criteria used, and receive any objections an

individual might make.

I now want to turn to matters of oversight and enforcement powers under PIPA. The question is what kind of powers are required in order to ensure rights and obligations set out in our legislation are actually met.

The first issue I want to discuss with you relates to my authority to enter into information sharing and cooperation agreements with other authorities.

The proposed CPPA will carry forward the existing PIPEDA authority for the federal Privacy Commissioner to enter into information-sharing and cooperation agreements with domestic and foreign privacy regulators. It also allows for such agreements with domestic regulators who have overlapping jurisdiction. Our law should mirror these provisions.

I cannot overstate the benefits of having a framework in place that supports collaboration between privacy regulators both domestically and internationally. At present, PIPA supports our domestic enforcement cooperation with other Canadian privacy regulators. We rely heavily on federal-provincial sharing and cooperation agreements as can be seen by recent joint privacy commissioner reports into Clearview AI, Cadillac Fairview, and LifeLabs.

However, PIPA does not explicitly extend these sharing arrangements to international partners, which is a problem at a time when many privacy issues are transborder in nature. I have encountered situations in recent years where it has been challenging to work together with privacy regulator colleagues outside Canada who wish to cooperate with us. You can assist greatly in these efforts by recommending language for our legislation that explicitly permits this. Similar explicit language would also better support my cooperation with domestic regulators, such as the Ombudsperson, Auditor General and Chief Electoral Officer, with whom I have worked in the past on matters involving personal information practices.

Again, these recommended changes will help align PIPA with the federal law and global trends.

Finally, I would like to turn to a recommendation that has come before the committee a number of times: the authority for my office to issue monetary penalties. There is little doubt that, if PIPA is to be considered substantially similar to the CPPA, PIPA's enforcement framework will have to be significantly strengthened. This includes authorizing my office to impose monetary penalties on organizations for breaches of the law.

The CPPA will do this by enabling the imposition of significant monetary penalties. Financial penalty provisions also align with the GDPR, the United Kingdom's *Data Protection Act, 2018* and Quebec's Bill 64.

As I noted in my briefing to the Committee last June, our joint investigation reports with the Office of the Privacy Commissioner of Canada, including one involving the social media giant Facebook, exposed the complete inadequacy of PIPA when it comes to protecting the public's personal information.

PIPA is, in many respects, toothless because the most I can do to sanction even a serious, wilful violation of our legislation is to order an organization to do what it should have done in the first place—fulfil its legal duty under the law.

My office has always emphasised an educational and remedial approach to compliance with the law and we will continue to do so.

But it is clear that there are bad actors out there who do not respect their duty to operate within legal boundaries and should therefore face monetary sanction. These kinds of penalties are always a last resort.

The need for these measures is widely acknowledged, as is illustrated by submissions made to the Special Committee last year. Among those supporting such measures were the Insurance Bureau of Canada and Canadian Bankers Association, as well as civil society groups such as the Canadian Civil Liberties Association, BC Civil Liberties Association and BC Freedom of Information and Privacy Association.

While the CPPA's power to impose monetary penalties is welcome, I do not support the adoption in BC of the CPPA's mechanism for doing that.

In short, the CPPA would create a new statutory tribunal, separate from the Privacy Commissioner's office that will have the exclusive authority to impose penalties, leaving the federal Privacy Commissioner to only recommend them. Creation of a new body to discharge this role is unprecedented in the Canadian privacy oversight world and in the EU context.

It would also run counter to the BC approach in other areas. As the Registrar of Lobbyists, for example, I have for some time had authority to impose monetary penalties under the *Lobbyists Transparency Act*. This authority extends to other regulators in the province as well.

There is no reasonable case to be made that the step proposed by the federal government is necessary in terms of institutional design in BC. The creation of a new tribunal would introduce unnecessary complexity, delay and uncertainty for individuals and organizations alike. It would also impose significant costs on the public purse and on those involved in disputes before my office.

I therefore continue to recommend that PIPA should enable the Commissioner to impose a monetary penalty on organizations for non-compliance with PIPA and that such authority be accompanied by strong provisions for due process and judicial oversight.

Conclusion

In concluding my remarks this afternoon, I can do no better than restate the message I gave to the Special Committee last fall: as law makers, as policy makers and as regulators, we need to work in tandem to keep up with the times. PIPA was drafted almost 20 years ago under very different conditions from those which we live under today. Rapidly evolving digital technologies, business models, and public attitudes toward privacy require us to respond in a way that is equal to the unique challenges we face.

Inaction is not a viable option. It simply is not.

Economies of the world are interlinked and so too is the flow of personal data that attaches to global trade. As a prolific trading jurisdiction, it is critical that we ensure that our personal information privacy laws are leading edge and, to the greatest extent possible, harmonized nationally and internationally.

I hope that through my submission and this presentation today I have shown how the GDPR, through its adequacy standard, has moved the Canadian government to propose enhanced privacy protection rules. This in turn reinforces the need for us in BC to do the same, to ensure we maintain substantial similarity with the federal legislation.

The recommendations my office made to the Special Committee in 2020 in many ways foreshadowed what the CPPA now proposes, and while PIPA and the CPPA need not be identical, it is in the interests of economic growth in the province, and citizens' privacy, for our law to be modern, robust, and balanced, while harmonizing with federal law and international developments.

I want to thank you again for your work on behalf of the citizens of British Columbia and for the opportunity to appear before you today. I welcome your questions.