Submission to the Ontario Ministry of Government and Consumer Services on Modernizing Privacy in Ontario

Canadian Life and Health Insurance Association
September 2021

Canadian Life & Health Insurance Association
Association canadienne des compagnies d'assurances de personnes

The Canadian Life and Health Insurance Association (CLHIA) is pleased to provide its comments to the Ontario Ministry of Government and Consumer Services on its white paper entitled *Modernizing Privacy in Ontario: Empowering Ontarians and Enabling the Digital Economy* ("white paper"). We would like to commend the government for engaging in dialogue with Ontarians on this issue prior to introducing any legislation. We believe there are key considerations that need to be taken into account before any legislative process.

The following submission is divided into two parts: the overview section provides general comments on the white paper for your consideration. The technical annex provides detailed responses to the questions provided in the white paper.

OVERVIEW

The CLHIA is a voluntary association with member companies which account for 99 per cent of Canada's life and health insurance business. The life and health insurance industry is a significant economic and social contributor in Canada.

$2.8 billion in provincial tax contributions

- **$210 million** in corporate income tax
- **$351 million** in payroll and other taxes
- **$592 million** in premium tax
- **$1.64 billion** in retail sales tax collected

Investing in Ontario

- **$337 billion** in total invested assets
- **98%** held in long-term investments

The industry also plays a key role in providing a social safety net to Ontarians.

Protecting 11 million Ontarians

- **10.2 million** with drug, dental and other health benefits
- **8.4 million** with life insurance averaging $234,000 per insured
- **4.9 million** with disability income protection

$46.8 billion in payments to Ontarians

- **$25.7 billion** in annuities
- **$16 billion** in health and disability claims
- **$5.1 billion** in life insurance claims paid

The life and health insurance industry has a strong interest in protecting the privacy of personal information. By law, full disclosure of relevant information is required to establish valid life and health insurance contracts and it is also needed in the assessment of claims for benefits (e.g., death claims, disability claims, medical or dental claims).

Canadians provide and trust insurers with their personal information. Protecting this information is a fundamental practice for insurers. Accordingly, the CLHIA and our member companies have historically taken a leadership role in the protection of personal information.

Harmonization

Many life and health insurance companies operating in Ontario do business across Canada. Having separate and potentially incompatible rules in Ontario will hinder their ability to operate in the province.

Introducing new provincial legislation will create uncertainty and increase regulatory red tape in Ontario, by:

- increasing administration and systems costs,
- reducing competitiveness and innovation, and
- overall make doing business in Ontario and across Canada more difficult.

This will be especially burdensome for small to medium size enterprises (SMEs) to learn and adapt to rules under a new provincial regime, while at the same time attempting to recover from the COVID-19 crisis. As Canadian governments and businesses begin to bounce back from the COVID-19 crisis and direct their efforts towards the economic recovery, it is essential that there be regulatory coordination across all jurisdictions so as not to impose an additional burden on businesses that have been financially impacted by the pandemic.

Many life and health insurers are still addressing COVID-19 issues by: working to help employers keep their employees connected with benefit plans; processing COVID-19 disability claims quickly; and also adjusting to the transformation in health care as virtual care allows services like physiotherapists and doctors to stay connected with Ontarians. The industry also continues to support communities that have been disproportionately affected by the pandemic. It is critical that supports for these communities continue, especially where access to all levels of health care resources, including supports for mental health, can be limited or non-existent.

For these reasons, we believe a new privacy regulatory framework in Ontario is not needed and instead, it is essential to ensure that modernization is coordinated with the federal government's framework for privacy. Our industry generally supports the direction established by the federal government in its recently tabled legislation (Bill C-11) to update the privacy framework because it:

- Maintains much of what works well in Canada – for instance, the Bill is principles based, technology neutral and focused on early resolution;
- Achieves advances in key areas, such as the inclusion of a new right to be informed of automated decision-making, business activities/innovation and a role for voluntary codes and certification;
- Maintains a focus on consent, where consent can be most meaningful, while also introducing practical exceptions to consent with parameters for business; and
- Ensures comparability to – or interoperability with – other jurisdictions, while also remaining tailored to our specific circumstances in Canada.

The direction of the federal government's framework for privacy is largely supported by the business community as it strikes a reasonable balance between an individual's right to control how their personal information is used and the reality that organizations often require personal information in order to provide new and innovative services to Canadians.

Should the Ontario government decide to move ahead with its own legislation in this area, we would strongly encourage the province to focus on areas that are currently not captured by the federal legislation. As noted within the consultation paper, the scope of the federal legislation is limited to commercial activities. Therefore, organizations such as charities, unions, associations, and other non-profits would not be covered. We support the province's approach to close the gap by creating privacy legislation in the province that focuses on oversight of these organizations to ensure Ontarians' personal information is adequately covered.

Supporting Innovation

Given life and health insurers' lengthy and active history in the protection of personal information, the industry has a strong interest in recent actions taken by governments to modernize or introduce new privacy legislation in Canada. We believe it is important to ensure that privacy frameworks reflect the increasing use and importance of data and the rapid pace of technological change.

Any coherent regulatory framework must ensure businesses are able to innovate and offer customized products and services that meet Ontarians' needs. Life and health insurers need to be given the ability to continue to develop ways to better meet the needs of their clients, whether by using innovative approaches to reduce costs for small businesses or by providing consumers with new products such as access to virtual health care. A coherent regulatory system will also help provide Ontarians with a clear understanding of how their information is used, rather than having to decipher a disjointed system that is inconsistent or unclear. That is why privacy frameworks must continue to balance the rights of Canadians to protect their personal information with the legitimate collection, use and disclosure of information by business for innovation and improving the lives of Canadians.

In fact, we believe that a robust approach to privacy protection is a necessary pre-condition for insurers to be able to innovate. We are fully aware that we must secure and maintain the trust of our clients by ensuring that their privacy is protected and that their data is secure. By doing so, we earn the trust of our clients to innovate with the data we hold in order to improve our services for them.

Process/Timing

Privacy legislation in Canada is important to ensure individual's personal information is protected while still allowing for new technologies and innovation that benefit consumers. It is important to get the legislation right as it could have a large economic impact and could hinder business in the province. The development of such legislation requires significant time and consultations in order to achieve an appropriate balance.

We understand that the Ontario government intends to move quickly on this issue and is aiming to draft and implement legislation in a very short period of time. We believe that having a short consultation period in the middle of summer on something so significant and important to the people of Ontario could result in insufficient feedback. We would caution the government on moving ahead too quickly and would strongly recommend that the government provide more time for businesses and individuals to fully understand the implications and potential consequences of a new provincial privacy framework.

CONCLUSION

The life and health insurance industry supports private sector privacy legislation that is harmonized across Canada and strikes a reasonable balance between an individual's right to control how their personal information is used and the reality that organizations often require personal information in order to provide services to consumers. We do not believe additional provincial legislation is required but rather that Ontario, and all provinces, should work with the federal government to continue to amend its federal legislation in a manner that would be take into consideration provincial concerns.

Should the province of Ontario see a need to otherwise protect its constituents, we suggest that the province focus on those areas not captured by federal legislation. Provincial legislation can complement existing federal legislation and close any gaps by creating privacy legislation that focuses on oversight of those organizations not covered by federal legislation to ensure Ontarians' personal information is adequately covered.

The industry greatly appreciates this opportunity to provide comments on the government's white paper. We have provided more detailed responses to specific questions in the white paper in the attached annex. Should you have any questions or require additional information, please contact Susan Murray, Vice President of Policy and Government Relations at smurray@clhia.ca.

TECHNICAL ANNEX: RESPONSES TO QUESTIONS ON PRIVACY WHITE PAPER

Rights-based approach to privacy

Does the proposed preamble in this section include the right principles, reasons and values to guide the interpretation of a potential privacy bill?

The goal of the preamble should be to set the tone for the legislation by establishing a framework for the protection and control of personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

he suggested preamble does not strike the balance required to reflect the values needed to guide future interpretation because it fails to recognize the coexistence of the privacy rights it wishes to establish with the legitimate business needs necessary to accomplish the activities that drive the province's economy.

This balanced approached was recognized under PIPEDA and has served us well over the years including the appropriate purpose requirement that can also be found in Federal bill C-11 under the CPPA as follows:

> *5 The purpose of this Act is to establish — in an era in which data is constantly flowing across borders and geographical boundaries and significant economic activity relies on the analysis, circulation and exchange of personal information — rules to govern the protection of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.*

We believe the purpose language in the CPPA captures this balance well and Ontario should use similar language.

How should the concepts of personal information, and "sensitive" personal information, be defined in law?

All concepts, specifically in privacy legislation, are closely interrelated. Consequently, we feel it is not possible to propose suggested language without having a full understanding of its intended use in the overall legislation.

However, since the concept of personal information already exists in Canadian privacy legislation, we suggest that any definition be harmonized with the federal legislation.

As for sensitive personal information, we recommend that you follow the approach adopted in the federal legislation and specify where requirements need to take into account the sensitivity of the personal information (e.g. privacy management program to take into account of sensitivity of information, sensitivity is a factor to consider when assessing appropriate purpose etc.) rather than providing a definition. A significant body of interpretation under PIPEDA exist with regards to the meaning of sensitive personal information. Adopting the suggested approach will retain the needed flexibility in determining what is sensitive by considering the nature and context around the personal information.

Do the "fair and appropriate purposes" proposed in this paper provide adequate and clear accountability standards for organizations and service providers?

PIPEDA has been based on the notion of reasonableness from its inception. Alberta's *Personal Information Protection Act* even contains a standard as to what is reasonable. Consequently, organizations from all industries are very familiar with it and, based on years of experience, understand it well. We are therefore questioning the need to introduce a different criterion which, in everyday language, appears to appeal more to a subjective sense of equity rather than one of well-established reasonableness. The suggested change is ambiguous and would introduce confusion in the analysis of the purpose and such uncertainty and lack of harmonization is not only undesirable but unnecessary. In addition, the introduction of a new concept may have significant unforeseen consequences including to restrict reliance on prior valid interpretation.

How far should the data rights of erasure and mobility extend? Should they include all information an organization has about an individual, or only the information the individual provided?

Any rights of erasure and mobility should be limited to information provided by the individual. The data independently developed by an organization based on information provided by consumers is a competitive asset that the organization has spent considerable resources developing and may include proprietary business information. Therefore, it must not be subject to any data mobility requirements. We consider derived information any information that the organization has developed to enhance its services and differentiate itself from others in their field (insights, observed data, processed data etc.). An example of derived information in the life and health sector is a profile or categorization of the risk of an individual pertaining to their life expectancy.

However, we acknowledge that the information subject to data portability should meet the primary objective of giving individuals control over information they have provided and that is included in a transaction. Therefore, information disclosed by the individual such as their status as a smoker or prior cancer occurrences, for example, would be considered as information that would be subject to portability. This information could, upon the consumer's request, be shared with another insurer to accelerate the application process which frequently involves the consumer consulting multiple insurers.

It is important however to understand that the concept of data portability is mainly about.

marketplace competition (easier access to goods and services) and that privacy is only one aspect of consumer protection that must be considered. Consequently, we do not believe that all the elements of the required infrastructure should be addressed in the legislation. Rather, the legislation should limit itself to permitting and protecting the sharing of personal information including guarding against fraudulent data requests. One way to do so could be to require that the request be made by the individual wishing to move their data directly rather than through the recipient third party. Consequently, no "bulk" demands, where an organization requests data for an individual from every competitor should be permitted.

In addition, the legislation must not require organizations to maintain technically compatible systems with all other organizations in order to facilitate a right to data portability. Any right to portability must be premised solely on computerized personal information and its sharing cannot raise serious practical difficulties. Separate sectoral frameworks could subsequently be developed with the help of industry associations to govern the technical aspects of data portability in different industries.

Any framework around rights of erasure or deletion, where individuals can require organizations to dispose of any their personal information, must be clearly outlined or privacy rules will frustrate organizations from meeting their regulatory or contractual obligations and possibly risk related liability or costs.

For example, in order to assess a claim for benefits, a life and health insurer must consult supporting medical information. If an individual requests that their personal information be deleted during the assessment process thereby negating the insurer's access to the necessary information, the individual must accept that it will be impossible for the insurer to process their claim. It would be unreasonable to allow this action from the individual to be deemed as a refusal by the insurer to fulfill its obligations.

These rights of erasure and deletion must therefore either be conditional on the fulfillment of already agreed upon legitimate purposes or the legislation must protect organization against regulatory or contractual risks that the individual's request might create and the exclusions must be expanded to include requirements under guidelines and decisions of federal and provincial regulators. For example, OSFI has several guidelines imposing records retention requirements on financial institutions. Specifically, guideline E-5 Retention/Destructions of Records states that "Claims records should be maintained for review by the Office. Sufficient records should be kept indefinitely to ensure that claims are not paid twice." Retention is also necessary in the context of fraud protection. There are additional examples in the life and health industry where those requirements exist and where the Ontario legislation, as contemplated, would put insurers afoul of the expectations of their regulators.

We further suggest that exclusion 1 (b) be clarified to reflect that the term of the contract does not need to directly address the disposition of information but rather that it would have for effect to keep information that would preclude any requests for disposal:

> "(b) there are other requirements of this Act, another Act or an Act of Canada or an Act or regulation of Ontario or Canada or of the reasonable terms of a contract that requires the organization to retain the information in order to fulfill those requirements;"

Otherwise it might be impossible for an organization to fulfill its regulatory and contractual obligations.

Such rights could also extend to information provided by them (see above) and held by third parties if organizations are permitted to comply with such requirements by contractual means.

As for a possible "right to be forgotten" we believe your suggested approach that it be clearly limited to a public online context is appropriate.

SAFE USE OF AUTOMATED DECISION-MAKING

Do the example provisions provided in this section offer adequate protection for Ontarians whose information is subject to ADS practices?

We believe the suggested provisions offer adequate protection for Ontarians. We are, however, concerned that, as drafted, these sections set an expectation that organizations must provide information that would be considered proprietary (e.g. trade secrets, business processes, algorithms).

We have provided comments to ISED under bill C-11, that the term "general account" raises some questions as to its meaning. We suggest it be replaced by the term "general description" which is more user friendly and may better reflect the intention of the legislator, that general information regarding the existing governance process is being provided.

In addition, the threshold of "significant impact" is ambiguous. We suggest that it be replaced to apply to a decision that could "produce legal effects on the individual or, similarly significant impact on them" which resemble the GDPR approach which is designed to address risks associated with ADS such as the fact that the process may be invisible, misunderstood or that information is used in ways unexpected by individuals.

In addition, we note that as currently suggested, the overall requirements applicable to automated decisions making does not in fact apply to the making of decisions but rather to all use of automated systems, including predictions and recommendations. This approach is too broad even when compared with the GDPR. Consequently, we suggest limiting the applicable requirements to a *decision* about the individual made with an automated system.

Requirements pertaining to automated decision processes should be limited to decisions based exclusively on such processes as the concept of assisted judgment is too broad.

We further recommend against introducing requirements that would provide a right of veto for individuals which would greatly limit innovation and have cost and time implications for all involved as automated decisions making tools often allow certain processes to be more rapid. We suggest that the contemplated introduction of a right to contest such decision doubled by the transparency requirements are the appropriate tools to ensure consumer protection.

Does the proposed regulatory approach for ADS strike the right balance to enhance privacy protections, while enabling new forms of socially beneficial innovation in AI?

We believe the balance reached is reasonable. However, we wonder if this approach will indirectly exclude as unacceptable other forms of AI that could be beneficial to society but may not meet the strict requirements of is the term “socially beneficial”. Consequently, we would like to see this approach extended to all AI innovations and not only to those as defined.

Should there be additional recordkeeping or traceability requirements to ensure that organizations remain accountable for their ADS practices?

We believe individuals can be provided with clear and accurate information with regards to their personal information without the need for additional recordkeeping or traceability requirements. In addition, we are concerned about how the notion of traceability will be interpreted as it may not be possible to comply if the technical requirements are too high. Such additional steps would add very little to the already existing accountability obligations or transparency provided by an organization and would not enhance protections for individuals while adding significant administrative and technical burden to businesses.

Are there additional requirements or protections that Ontario may consider related to the use of profiling?

We do not believe that additional requirements or protections are required to supplement what federal bill C-11 would introduce. However, we would be interested in discussing any suggestions that might emerge with regards to enhancing transparency.

ENHANCING CONSENT AND OTHER LAWFUL USES OF PERSONAL INFORMATION

Does the sample list of “permitted categories” provide a sufficient set of authorities for the collection, use and disclosure of personal information? Are there any categories missing? Are there any categories that are too permissive?

In order to ensure harmonization with the federal legislation, we suggest that additional permitted categories be added such as Information produced in employment, business or Profession (s. 23 bill C-11), Disclosure to lawyer or notary (s. 25 bill C-11), Witness statement (s. 26 bill C-11) and Debt collection (s. 28 bill C-11).

We have no objections to the category entitled "investigation or legal proceedings" if it is clarified that an investigation includes the prevention of fraud. This clarification will be of crucial importance for the life and health industry.

We believe the permitted category of "Research and development" should be expanded to address other legitimate practices. In some circumstances, such as actuarial calculations, statistical research and pricing, the effectiveness of the research will require the use of internal datasets containing some personal information. However, this does not appear to be possible under the legislation Ontario is contemplating and would have a significant impact on the life and health industry

Therefore, we ask that an exception be introduced for these purposes, or alternatively that an additional activity specific for our industry be added to the list of business activities to be set by regulation as follows:

> *"**(1)** an activity that is carried out to understand and analyze the interests, needs and preferences of customers and users;*
> *(**2**) an activity that is carried out to assess, develop, enhance or provide products and services"*

A very important provision for the life and health industry is missing from the list of permitted categories, namely the use of the implicit consent of an individual in the context of insurance. For example, group insurance is insurance in which the lives, well-being or employment income of individuals who enroll under the group insurance contract are insured severally under a single contract between an insurer and an employer, creditor or other person.

Group insurance is not offered by the insurer directly to individuals. Rather, a plan sponsor (also known as a group policyholder) contracts with an insurer to provide coverage for its plan members (also known as participants). The plan sponsor then enrolls the individual members under the group insurance contract. A common example of group insurance is the life, disability, health and dental benefits many employers provide to their employees through a group insurance contract.

Unlike in the individual insurance context where more than one person can apply for joint coverage under a single policy, in the group insurance context only the individual (e.g. an employee) directly connected to the plan sponsor (e.g. an employer) may apply for enrollment under the group insurance contract. If the application is accepted, the individual becomes a plan member, also known as the group person insured, under the group insurance contract. Any other individual associated with the plan member, for example a spouse or child, would be considered a dependent under the plan member's coverage if eligible under the terms of the contract.

In this regard, the Ontario *Insurance Act*, R.S.O. 1990, c. I-8 ("*Insurance Act*") explicitly sets out that the rights under the group insurance contract belong only to the plan member, and not to the dependent. Hence, the coverage under a group insurance contract is that of the plan member and not that of the dependent. Consequently, the right to obtain coverage for a dependent belongs to the plan member and not to the dependent. A dependent's ability to be covered under a group insurance contract is subordinated to the plan member's willingness to extend coverage for his/her dependent under the plan member's coverage.

As insurance contracts are contracts of utmost good faith, the applicant has an obligation and responsibility to answer all medical or lifestyle questions accurately and to provide correct and current information when applying for coverage. Given that the coverage belongs to the plan member (and not to the dependent), should there be fraud or misrepresentation in the application related to the dependent's answers, the insurer would generally seek recourse against the plan member, not against the dependent, and could void the member's coverage for the dependent.

Consequently, we ask that you introduce a section that will clarify the requirements under the insurance legislation, from a privacy perspective, that an individual is deemed to consent to the collection, use or disclosure of personal information by an organization for the purpose of the person's enrollment for coverage under an insurance contract similar to the one under British Columbia's *Personal Information Protection Act* as follow:

> *8 (…)*
>
> *(2) An individual is deemed to consent to the collection, use or disclosure of personal information for the purpose of his or her enrolment or coverage under an insurance, pension, benefit or similar plan, policy or contract if he or she*
>
> *(a) is a beneficiary or has an interest as an insured under the plan, policy or contract, and*
>
> *(b) is not the applicant for the plan, policy or contract.*

Consider the sample "business activities" provision provided above. Is it properly balanced to protect personal information while allowing businesses to conduct their operations? How should Ontario define the concept of "commercial risk"? Should "any other prescribed activity" be removed from the list of business activities?

We believe the sample provisions with regards to "business activities" are well balanced, subject to our comment with regards to research and development above.

We do not believe that the concept of "commercial risk" should be defined because a specific definition may not apply in the context of all industries unless it includes common denominators such as the possibility of financial losses by the organization based on, amongst other things, the value of currency, strategic decisions, debtor dues. However, we bring to your attention that even a general definition such as the one suggested would not be fitting in the context of not for profit entities that we understand you intend to include in the scope of the legislation.

The possibility to have other prescribed activity by regulation should not be removed as the legislation must have some flexibility to address efficiently any situation that was not taken into consideration or did not exist when it was drafted. This is especially true when we consider the rapid progress of technology and therefore, we do not want the legislation to be obsolete in that aspect quicker than the province can update it.

In addition, we recommend that the section 1(b) be modified to restrict this requirement to situations where the "sole or primary" purpose is to influence the individual's behaviour or decision making, such as targeted behavioural marketing.

We suggest that these provisions be subject to the knowledge or consent of individual to ensure appropriate harmonization with the federal legislation.

Are there any additional protections or requirements that Ontario should consider in respect of service providers?

We have no additional protections or requirements to suggest but would like to raise for your consideration the confusion that may stem from the use of two different terms in sections 1) and 2) with regards to the disclosure and use of personal information by a service provider. The provisions allow an organization to *disclose* personal information to a service provider and, in return, the service

provider may use such information *transferred* to them by the organization. We suggest that use of the word "disclosure" in subsection (1) be replaced by "transfer" since a transfer of information is a use by the organization which is, as stated by the OPC[1] "not to be confused with a disclosure."

> ***Disclosure to service provider***
>
> *(1) An organization may ~~disclose~~ transfer an individual's personal information to a service provider.*
>
> ***Use by service provider***
>
> *(2) A service provider to which personal information has been transferred by an organization may use the information only for the same purpose for which it was collected by the organization.*

Also, we suggest you carefully consider the use of services providers in other jurisdictions (i.e. cross-border transfers). Organizations should be able to transfer personal information across borders without consent.

DATA TRANSPARENCY FOR ONTARIANS

Is the "privacy management program" requirement sufficient to ensure that organizations are accountable for the personal information they collect?

We believe the suggested requirements for the establishment of a privacy management program are reasonable and feasible. We have no suggested changes to present.

Are the sample provisions in this section sufficient to ensure that Ontarians understand the nature, purpose and consequences when an organization collects or uses their personal information?

We believe the sample provisions are sufficient. However, some requirements raise questions and others concerns. Section (3) 2 i. should be more precise and indicate that the right of withdrawal is subject to applicable law or reasonable contractual terms. This would clarify that situations exist where an organization may no longer be able to provide the requested service should the individual withdraw their consent. Once more, the example we submitted on page 3 of this document is helpful. In order to assess a claim for benefits, a life and health insurer must consult supporting medical information. If an individual withdraws their consent thereby negating the insurer's access to the necessary information, the individual must know that it will be impossible for the insurer to process their claim.

With regards to section (3) 2 ii, we wonder what is the expectation to "record" the purpose?

We find the interpretation of the expression "foreseeable consequences" to be very broad and ambiguous. We are concerned that it may be misunderstood and captures too many situations. We would ask that, at a minimum, guidance be provided on the matter before any related requirements come into force.

We also wish to ask for clarification with regards to subsection (3) 2 v which requires the disclosure of the "specific" type of personal information that is collected to the individual. Since the requirement is only applicable at or before the time of collection, we are wondering why, while the organization is

[1] Processing Personal Data Across Borders Guidelines p. 5

asking an individual's medical information, to disclose that this information they are currently collecting is of a medical nature.

Should Ontario consider a mandatory requirement for "Privacy by Design" practices or "privacy impact assessments"? What kind of burden would this kind of requirement cause for organizations? How should Ontario balance the value of these requirements with this potential burden?

Although we understand the purposes of these suggested approaches, we question the ability of organizations of all sizes to understand and/or have the capacity to implement these concepts which may not be familiar to them. We believe there is a significant need to educate businesses before mandatory requirements can be considered.

In addition, to adequately conduct a privacy impact assessment involves significant resources. Should requirements be introduced to make them mandatory, they must apply for the future only, be limited to technical projects having significant impact and involving a reasonable amount of personal information. In other words, the need to conduct an assessment must be based on principles of proportionality and materiality, taking into account the amount and degree of sensitivity of the personal information, the nature of the issues and the size of the company.

PROTECTING CHILDREN, YOUTH AND VULNERABLE INDIVIDUALS

Should Ontario consider other requirements to enhance protections for other vulnerable populations, such as seniors and people with disabilities?

We believe this important topic is better left to representatives of these populations to comment. Financial institutions' regulators have been establishing guidance on the protection of vulnerable individuals and we have been working with them to develop solutions that can be operationalized. We suggest once more that this is an aspect of the legislation that would benefit from a harmonized approach for organizations to be allowed to provide the same level of protections to all affected populations.

We also bring to your attention section 7(3)(d.3) of PIPEDA which provides an organization some tools to protect victims of financial abuse. It has been extensively debated and was introduced as an amendment following advocacy efforts on the part of financial institutions.

A FAIR, PROPORTIONATE AND SUPPORTIVE REGULATORY REGIME

Would certification programs and codes of practices be effective in proactively and collaboratively encouraging best practices in privacy protection?

Our industry would be interested in additional mechanisms that allow organizations to proactively demonstrate compliance with privacy legislation provided they are effective. The public must clearly understand that a recognized authority supports these accountability protections.

We believe codes of practice and certification schemes should be voluntary and their cost should not be prohibitive. Otherwise, cost could be a barrier to new entrants or smaller players seeking to comply with standards. Third party certification must be recognized by the Commissioner to ensure that adherence protects organizations against certain enforcement activities or, at a minimum, eases the burden of any privacy audit or investigation process.

Any review process must also be agile. The goal should be to demonstrate that the organization meets certain privacy standards rather than to engage resources in filling out an annual questionnaire. There should also be an escalation process in the event that the organization does not agree with the result of the review, which should not ultimately be overseen by nor involve the initial reviewer.

We believe voluntary codes of practices can play an important role in enhancing transparency and accountability practices in the context of privacy. However, to be truly effective, they should be specific to each industry and therefore written by, or having substantial involvement from, each industry association. This will ensure the codes are meaningful in the context of each industry's business realities. In addition, codes of conduct are low cost and allow the flexibility required to adapt to new business practices and rapid technological changes.

One important incentive will be to ensure an organization is protected against certain enforcement activities and/or that the burden of any privacy audit or investigation process with regards to the codes/certification scheme is lessened. If the mechanism works well, these tools must serve to demonstrate the organization has already met a determined level of accepted standards to both the reviewer and the general public.

A company's public declaration that it follows a privacy code or has had its privacy practices certified also encourages them to follow these standards with care as any deviation could have significant impact on its reputation.

Are administrative monetary penalties effective in encouraging compliance with privacy laws? Are the financial penalties set at an appropriate level?

The Commission's structure is not well suited to fulfill the functions of support to organizations, complaint resolution, and proactively undertake investigations as well as reviewing decisions and levy fines. These additional functions would undermine the Commissioner's key role as a support to businesses which fulfills an important task in keeping open the lines of communication between the Commission and industry stakeholders.

However, should government introduce administrative monetary penalties to a private sector privacy legislation, we believe a third party should be incorporated to mediate this mechanism and that, at a minimum, administrative monetary penalties be viewed as a regulatory offence, to ensure that the rules of administrative law apply (e.g. procedural fairness including a proper appeal or escalation process on matters of facts, law or quantum), be exercised only in limited instances of egregious behaviours and where the quantum is based on a demonstrable relationship between the violation and the harm. Specifically, as currently presented in the consultation paper, it appears that only matters of law would be heard on appeal. Considering the importance of the potential penalties, we believe that questions pertaining to the quantum should also be grounds for appeal.

In addition, serious consideration should be given to the possibility that those fines and penalties may be awarded in more than one jurisdiction. In such case, a coordination process between provincial and federal privacy commissioners will be key to manage any conflicts. Given that Canada already has more than one privacy regime, it is conceivable that an organization could be fined up to five times across the various jurisdictions for the same actions. Clearly, this cannot be the intent of these frameworks, and every effort should be taken to avoid such outcomes.

Would the ability for the IPC to issue orders requiring organizations to offer assistance or compensate individuals be an effective tool to give individuals quicker resolutions to issues?

We would like to obtain clarification as to the meaning of "offering assistance". What would the expectations following such an order be?

SUPPORTING ONTARIO INNOVATORS

Would the clearer articulation of which privacy rules apply to de-identified information, as discussed in this section, encourage organizations to use de-identified information, and therefore reduce privacy risk?

We believe that the clearer articulation of the rules that apply to de-identified information could be useful. However, these rules are only useful if the expectations are the same across Canada since it will be impossible for organizations to build appropriate infrastructure for each province and to meet different requirements (especially if they are contradicting) when information crosses provincial borders.

Would the inclusion of the concept of anonymized information, and clarifying that the privacy law would not apply to this information, encourage organizations to use anonymized information?

We believe that an attainable definition of anonymized information could encourage the use of anonymized information and promote innovation. However, as noted above, the same criteria must be used across Canada and cannot be contradictory. Organizations will be unable to implement processes that may not be compliant in all Canadian jurisdiction. Otherwise, we believe that organizations could rely on reasonable industry standards.

For sharing information for socially beneficial purposes, what additional safeguards or governance would be needed in addition to de-identification of information, in order to protect privacy?

As noted above, we believe that more initiatives should be permitted to qualify as socially beneficial.

79 Wellington St. West, Suite 2300
P.O. Box 99, TD South Tower
Toronto, Ontario M5K 1G8
416.777.2221
info@clhia.ca