Submission to Consultation on Open Banking

Prepared by the BC Freedom of Information and Privacy Association for submission to the Advisory Committee on Open Banking, Department of Finance Canada

October 11, 2019

BC Freedom of Information and Privacy Association
103 – 1093 West Broadway
Vancouver, British Columbia, V5N 1E2
Phone: 604-739-9788 | Fax: 604-739-9148
fipa@fipa.bc.ca

Introduction

This submission was prepared by the B.C. Freedom of Information and Privacy Association ("FIPA") in response to the consultation document, *A Review into the Merits of Open Banking*, from the Ministry of Finance.

FIPA is a non-partisan, non-profit society that was established in 1991 to promote and defend freedom of information and privacy rights in Canada. It is based in Vancouver, B.C. and aims to empower citizens by increasing their access to information and their control over their own personal information. FIPA has served a wide variety of individuals and organizations through programs of public education, public assistance, research, and law reform. It is one of the very few public interest groups in Canada devoted solely to the advancement of freedom of information (FOI) and privacy rights.

We thank the Ministry of Finance for this opportunity to discuss issues relating to data and finance and its intersection with privacy rights.

We have read and understood the consultation procedures and we hope you will find this submission helpful.

Summary

This submission will present a brief discussion of the Canadian privacy and data protection framework. It will then provide a comparison of Canadian data protection regulations with other international regulations, such as the General Data Protection Regulation ("GDPR") recently implemented in the European Union ("E.U."). This is followed by a discussion on the impacts that open banking will have on individual privacy rights, by utilizing recent examples of digital transformation across Canada. Finally, this submission will outline several practical considerations for open banking within Canada before concluding with a list of key recommendations to consider moving forward.

Our main recommendations are:

1. FIPA recommends that funding is increased for education and awareness campaigns to inform the public about potential risks of open banking and available remedies in the event of privacy breaches.
2. FIPA recommends the Canadian government works to implement a proactive reporting culture in organizations and positive treatment of privacy rights that is led by educated individuals.
3. FIPA recommends that the Canadian government works with the Privacy Commissioner and Office of Privacy to develop an accessible complaints process for individuals to report privacy breach concerns.
4. FIPA recommends that the Canadian government increases funding to the Privacy Commissioner and the Office of Privacy. Further, FIPA recommends that the investigative and enforcement powers of the Privacy Commissioner and Office of Privacy are strengthened through legislative amendment, like current data protection and privacy legislation in British Columbia.
5. FIPA recommends that the Canadian government take proactive steps to research and study the impacts that privacy issues in open banking will have on marginalized groups.
6. FIPA recommends that the Canadian government develops a new data protection and privacy framework to comply with open banking and allows enough time for interested groups to provide feedback prior to implementation.

The Canadian Privacy Landscape

The Canadian privacy landscape is represented by a mix of Federal and Provincial legislation linked by policy and a list of fundamental principles. The Federal Acts, which consist of the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* (known as "PIPEDA") focus primarily on the use, collection and disclosure of personal information in Canada, and the limitations thereof, in relation to commercial activity.

In recent years, privacy advocates have petitioned for amendments to these Acts, arguing that the Acts are outdated and overly broad, and as such, not adequately protecting individual consumers' privacy interests. There is some truth to this sentiment, with the *Privacy Act* being introduced in 1983 and not undergoing any significant change since its inception. In contrast, PIPEDA was implemented in 2001 and has undergone several changes to keep apace with the evolving

consumer landscape. The most recent amendments to PIPEDA have been made through the enactment of the Digital Privacy Act in June 2015 and the breach reporting regulations that took effect in November 2018[1]. However, these amendments may not be sufficient in this era of global digital transformation, and individual consumers may not be adequately protected to withstand the changing economic tides.

In the private sector, PIPEDA was implemented on underlying "fair information principles"[2], which includes the requirement for individual consent prior to the collection, use and disclosure of personal information. The concept of consent is a key factor in protecting individual privacy rights and is an important consideration in the evolving digital marketplace. To ensure that Canadian regulations are protecting consumers, there must be strict requirements for obtaining informed consumer consent and implementing strict penalties where breaches occur.

In contrast to the *Privacy Act*, *PIPEDA* has been amended several times since its inception in 2000, to keep apace with the rapidly evolving digital economy and in line with its internal review mechanisms. Several groups have argued, however, that these amendments have been insufficient, as PIPEDA continues to suffer from almost immediate obsolescence by ongoing changes in the private digital economy. The OPC, along with other public organizations have been forwarding recommendations for changes to PIPEDA to overcome these challenges of overtaking digital forces.

In September 2017, the Privacy Commissioner of Canada, Daniel Therrien, held a news conference relating to the state of privacy laws within Canada[3]. He expressed a concern that the legislative tools available to Canadian consumers are insufficient to ensure adequate protection for personal data and individual privacy rights. He further expressed concerns that Canada is failing to keep up with international peers in the data protection arena. As it stands, Canadian regulations are out-dated and unable to effectively protect personal information.

In a world where digital transformation is ongoing, the standard of data protection and individual privacy rights within Canada must remain a priority for the Canadian government. Currently, the standard of privacy protection in Canada is too broad and ineffective to protect individual

[1] The new breach reporting regulations are published online at: http://laws-lois.justice.gc.ca/eng/acts/P-8.6/nifnev.html.
[2] These principles can be found at: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/ along with a toolkit for businesses on how to comply with PIPEDA.
[3] See a discussion of the conference at: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2017/nr-c_170921/.

consumers from the risks of open banking. The Canadian data protection regulations must be updated to instigate proactive reporting culture in organizations, increase the accessibility for individual consumers and to comply with international standards. The risk of maintaining inadequate privacy protection is not only a risk of privacy and data breaches, but also the potential limitation of business competitiveness in the modern global economy.

International Comparisons

European Union

The most recent notable change in data protection regulations is the *General Data Protection Regulation* ("GDPR") that came into effect in the European Union ("E.U.") on May 25, 2018. The GDPR provides an immediate standard by which to measure privacy and data protection in an innovative landscape. By reviewing the path that the GDPR has taken thus far, other countries may identify more efficient means to protect individual privacy rights within an open banking framework. Although GDPR gained significant criticisms when first passed in 2016, following the Facebook / Cambridge Analytica revelations last year, strong support has risen in relation to its enforcement.

The GDPR has a wider scope, more prescriptive standards, and substantial fines to strengthen data protection and individual privacy rights. The GDPR has also implemented mandatory breach reporting requirements in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals"[4]. Specifically, the GDPR applies not only to organizations within the E.U., but to global organizations that either have some physical presence in the E.U., actively target individuals in the E.U., or use intrusive technologies from abroad to interfere with individual privacy within the E.U.

The GDPR was first put forth by the European Commission in 2012 and generally agreed upon by the European Parliament and Council in December 2016. Although the GDPR went through many amendments within this time, global organizations were continuously updated on the significant impacts that such a regulation would have on the marketplace and were urged to

[4] *A new era for data protection in the EU, What changes after May 2018.* European Commission. https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf.

prepare for the changes that lie ahead. In 2016, Dell Technologies completed a survey on awareness and preparedness for the implementation of the GDPR and found that more than 80 per cent of global respondents knew few details or nothing about the GDPR and 97 per cent did not have any plan in place[5].

Since the GDPR came into effect on May 25, 2018, the chaos and confusion for global organizations has not lessened. Several smaller tech companies with data-driven business models chose to cease activities completely prior to the GDPR implementation date, acknowledging that they would not survive in a post-GDPR world[6]. For those who continued business in the face of the GDPR, many U.S. based companies, such as Tronc Inc., Lee Enterprises and GateHouse Media resorted to blocking E.U. readers from its online newspapers, to ensure that their activities were not subject to GDPR compliance regulations. Furthermore, many organizations chose to forego the high cost of altering their current business practices to conform with GDPR requirements and withdrew from the jurisdiction altogether. As of August 7, 2018, there were still hundreds of U.S. websites blocked in the E.U. due to non-compliance with the GDPR[7].

The number of data protection complaints, questions and breach notifications have also risen sharply, with local data protection authorities across the E.U. being flooded within days of GDPR implementation. The number of complaints received were highest in the United Kingdom, with 1,124 complaints being received within 26 days[8]. The estimated budget per complaint in the United Kingdom was approximately $1,468. The number of complaints is expected to stabilize as organizations become more familiar with the new regulations. However, there is no way to truly know the long-term impacts of the GDPR at this point.

The practical implications of GDPR have been felt internationally, with concerns related to trade restrictions being prominently raised by Wilbur Ross, United States Commerce Secretary earlier

---

[5]Dell Technology. *Dell Survey Shows Organizations Lack Awareness and Preparation for New European Union General Data Protection Regulation (GDPR).* October 11, 2016. https://www.dell.com/learn/us/en/uscorp1/press-releases/2016-10-11-dell-survey-shows-organizations-lack-awareness.

[6] Cerulus, L. and Scott, M. *Who stands to lose most from Europe's new privacy rules?* May 23, 2018. https://www.politico.eu/article/the-gdpr-hit-list-who-stands-to-lose-from-europes-new-privacy-rules-facebook-google-data-protection/.

[7] South, J. *More than 1,000 U.S. news sites are still unavailable in Europe, two months after GDPR took effect***.** August 7, 2018. NiemanLab. http://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/.

[8] Choudhari, J. *Cataloging GDPR complaints since May 25*. June 25, 2018. International Association of Privacy Professionals. https://iapp.org/news/a/cataloguing-gdpr-complaints-since-may-25/.

this year[9]. The U.S. Commerce Secretary commented that the GDPR in its current state *"…could significantly interrupt transatlantic co-operation and create unnecessary barriers to trade, not only for the US, but for everyone outside the EU.*" This statement was made in response to the GDPR imposing its reach outside the E.U. borders to include companies that are primarily based in other countries, such as Canada and the U.S. Through GDPR's broadened scope, many other countries have been forced to review their own data protection laws in a bid to catch up and stay current on international standards.

United States

The United States have come under pressure in the recent years regarding their own data protection and privacy legislation, especially in wake of the Yahoo data breach in 2016. This breach was referred to as the largest data breach in U.S. history, with the data of approximately 500 million user accounts reportedly stolen[10]. In response to this breach, Richard Blumental, U.S. Senator for Connecticut, released a statement urging Congress to enact data breach and security legislation by stressing that *"…only stiffer enforcement and stringent penalties will make sure companies are properly and promptly notifying consumers when their data has been compromised"*[11]. Even though these statements were made to convince the U.S. government to consider upgrading its privacy protection protocols, no changes have been made to date. In wake of the GDPR, the U.S. is now struggling to keep up in this rapidly changing arena. If the U.S. does not make a compromise, business operations may continue to weaken with the E.U.

Canada

In comparison to these global leaders, the Canadian government has passed the new breach reporting regulations that came into effect in November 2018[12]. The new regulations strengthen privacy breach notification protocols to ensure that individuals are promptly informed if their

---

[9] Roass, W. *EU data privacy laws are likely to create barriers to trade.* The Financial Times. May 30, 2018. https://www.ft.com/content/9d261f44-6255-11e8-bdd1-cc0534df682c.

[10] Fiegerman, S. *Yahoo says 500 million accounts stolen.* September 23, 2016. CNN. https://money.cnn.com/2016/09/22/technology/yahoo-data-breach/index.html.

[11] Blumenthal, R. *Massive Yahoo Hack Demonstrates Urgent Need for Congressional Action on Data Breach and Security.* September 22, 2016. https://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-massive-yahoo-hack-demonstrates-urgent-need-for-congressional-action-on-data-breach-and-security.

[12] The Order in Council for these amendments and fixing of the November 1, 2018 due for enforcing these rules can be found at: http://orders-in-council.canada.ca/attachment.php?attach=36009&lang=en.

information is at risk and that organizations must keep stringent breach records[13]. These regulations represent a significant change for commercial activities across Canada and come into line with some of the newly adopted rules under the GDPR. However, the Canadian regulations will need further amendment to promote more prescriptive standards for data protection, similar to the GDPR.

Canadian Examples of Digital Transformation

The emergence of new technology and increased methods of human interactions has caused a slew of entities to make innovative changes that are not bridled by legislative protections. There have been several incidents globally that have illustrated the emerging gap between the digital marketplace and the laws that try to protect our individual privacy rights and data. These incidents provide a means to re-evaluate our current privacy protection to ensure we are evolving with the digital landscape.

Facial Recognition Technology, Alberta

In recent months, the Privacy Commissioners of Alberta and Canada have launched investigations into the use of facial recognition technology at two malls in Calgary, Alberta[14]. It was reported by individual consumers that the malls were accessing several data points of shoppers to create an entire profile without their knowledge. The main concern about the use of this technology is the lack of information provided to consumers about collection of their data and the lack of consent from consumers. In response to the Privacy Commissioner's investigations, Cadillac Fairview decided to suspend use of the technology pending the outcome of their investigation[15]. However, there are no regulations in place within Canada to impose strict or severe sanctions on organizations for these kinds of privacy breaches.

Connected Cars, Canada

[13] Taillefer, C. Director of Privacy and Data Protection Directorate, http://www.gazette.gc.ca/rp-pr/p1/2017/2017-09-02/html/reg1-eng.html.
[14] A news release was posted on the website of the Office of the Information and Privacy Commissioner of Alberta (August 3, 2018): https://www.oipc.ab.ca/news-and-events/news-releases/2018/announcement-commissioner-initiates-investigation-into-the-use-of-facial-recognition-software-at-calgary-malls.aspx.
[15] This was reported in Global News on https://globalnews.ca/news/4372306/cadillac-fairview-suspends-facial-recognition-cameras-calgary/.

There have been other incidents that have also raised concerns about the standard of privacy protection in recent years. The incidents suggest that there have been no positive steps towards strengthening privacy rights in recent years. The use of connected cars and their disclosure of personal information was reviewed in 2015 and found to be in breach of data protection laws and infringing on personal privacy[16]. Several recommendations were put forward, including industry specific implementation of PIPEDA, to appoint privacy officers and to review consent mechanisms. To date, the industry has still not made these significant changes. This prompts questions to be raised about the willingness of organizations to institute data protection changes if those changes are not required under regulation.

Smart City, Ontario

These past examples are important to consider when contemplating the technological changes that are projected to occur in Toronto in 2020. To *"…conserve energy, cut costs and increase land efficiency"*[17], Sidewalks Labs, a company under the Alphabet Inc umbrella, announced plans to pilot a smart-city in Toronto's Quayside in 2020[18]. The project would be a completely digital city featuring autonomous vehicles, a thermal grid and robotic delivery and waste-management systems. These types of technologies would incidentally collect and use personal information as a means of improving quality of life and help the city learn from its inhabitants and would require strict compliance with data protection regulations.

This project has attracted a significant amount of scrutiny from professionals concerned about the impact of this project on individual privacy rights. At its current point, data protection regulations are too broad to adequately protect individual privacy in a projected smart city design. However, in response to recommendations by federal and provincial Canadian privacy regulators, Sidewalk Labs developed a Responsible Data Use Policy to guide the use of data in the smart city[19]. This policy was released with the intention that it would be a 'living document' that evolves through consultation with privacy professionals and the public. It includes

---

[16] BC Freedom of Information and Privacy Association, *Connected Cars:* 2015
[17] Saminather, N. *Alphabet unit to start Toronto smart-city tech pilot in summer, build in 2020.* April 9, 2018. Reuters. https://www.reuters.com/article/us-alphabet-canada/alphabet-unit-to-start-toronto-smart-city-tech-pilot-in-summer-build-in-2020-idUSKBN1HG2WS.
[18] Sidewalk Website documenting the project: https://www.sidewalklabs.com/.
[19] Version 0.2 of the Responsible Data Use Policy can be found at: file:///C:/Users/admin/Dropbox%20(RWE%20Law)/Samantha's%20Clients/FIPA%20Privacy%20SD/Articles/Sidewalk-Toronto-Responsible_Data_Use_Framework_V0.2.pdf.

commitments to inform individuals about the collection and use of personal information, to obtain informed consent and not to sell any personal information. This kind of policy, although necessary for developing smart cities, could be readily applied to other forms of digital transformation like open banking. The smart city may represent a valuable model for achieving balance between data protection regulations and private organizations, bridging the gap between the current legislation and its practical application.

There are some concerns to note in ongoing smart city initiatives that have been raised by global privacy advocate groups. In a report completed in 2017, Privacy International discussed the possible human rights breaches that could occur in a space under surveillance, such as a smart city, where individuals and their actions were constantly monitored and tracked[20]. The report discussed practical problems occurring within a smart city pilot in Jakarta, Indonesia. Even with very strict privacy and data protection regulations in place for the smart city, prevalent issues arose in Jakarta, such as the individual manipulation of collected data and a preference for use of data over personal feedback on services. Specifically, individuals would look to data in making important decisions instead of considering peer feedback. These concerns must be considered when embarking on a smart city within Toronto and adopted into Sidewalks Responsible Data Use Policy.

These recent examples of digital transformation within Canada provide a means to measure the level of awareness surrounding the collection and use of personal information in Canada. The level of public awareness has arguably increased, with incidents like the Calgary Mall being recognised and reported by individuals for investigation. The concepts of responsible use and collection of data and personal information are being brought to the forefront of consumer focus. This demonstrates a potential for forward movement in digital transformation across Canada without gross breaches of individual rights. If the public can continue to be educated and informed about protecting their personal information and digital practices, there is a potential for gradual digital transformation.

Private Companies, Privacy Policies, and Consent

[20] Privacy International. *Smart Cities – Utopian Vision, Dystopian Reality*. October 2017.

Currently, data protection and privacy regulations require organizations to create privacy policies that describe how they collect, use and disclose their consumers' personal information. These privacy policies are designed to act as tools to inform consumers about their privacy rights prior to consumers providing their consent. However, many consumers reportedly skip past these privacy policies blindly, without taking the time to inform themselves about the use of their personal information.

Following the discussion paper released by the Office of the Privacy Commissioner of Canada ("OPC") in May 2016 on the topic of consent, findings demonstrated a clear lack of informed consent within the digital marketplace. The findings also suggested that daily consumer transactions were rife with undue influence[21]. Most consumers stated that they were not reading the privacy policies they were presented with online and were blindly accepting terms relating to personal information collection and use. Therefore, the quality of consent gained by organizations is questionable and the actual level of control that consumers have over their personal information is illusory at best.

In response to a public opinion survey completed for the federal Office of the Privacy Commissioner in 2016, although 52% of Canadians believed they had sufficient knowledge about how changing technologies affect their personal privacy, 74% of Canadians thought they have less protection over their personal information now compared to 10 years ago[22]. Therefore, even though Canadians appear to be more knowledgeable about their privacy rights in the current technological climate, they are not confident that their rights are adequately protected. Further public discussions must be initiated to ensure that individuals are better informed about their privacy rights and their options to protect these rights in the future.

Personal Information, Privacy, and Complaints

The number of privacy breaches reported to the Privacy Commissioner has increased over the years, indicating that individuals have become better informed about reporting potential privacy

[21] *Office of Privacy Commissioner* 2015-16 Annual Report: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/#heading-0-0-4-1.
[22] The Report was published online at: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por_2016_12/.

breaches. Some privacy matters have been escalated to the Supreme Court and represent a range of issues surrounding consent and the collection/use of personal information.

A good example of an individual exercising their data protection rights is in the case of *Douez v Facebook, Inc.*[23] In *Douez,* a Facebook user, Deborah Douez brought an action in British Columbia against Facebook for the use of her name and likeness for advertising purposes without her consent. The proposed class affected by the breach was estimated to be more than 1.8 million people[24]. However, only a small number of members in the affected class were aware of the potential breach and able to commence an action to protect their individual rights and hold Facebook accountable. In this case, a small number of informed individuals were able to bring a class action on behalf of the majority. However, it does account well for marginalized groups within society who may be uninformed and unable to identify privacy breaches. The *Douez* case suggests that knowledge of reporting procedures for privacy breaches is not wide spread in the Canadian population. It further suggests that only members of a largely effected class will benefit from privacy and data protection regulations now and in the future.

For breach reporting tools to be widely utilized within Canadian society, they must be accessible on an individual level. This will assist smaller marginalized groups to keep informed and access remedies for privacy and data protection breaches. The practical effects of privacy and data protection regulations should not just operate for the protection of large classes, but also for individuals. The practical considerations in preparing for changes in a digital transformation to open banking must include increased funding for the education of consumers regarding data protection and privacy rights.

Considerations

A digital transformation to open banking that changes a country must start from a responsible and well-informed government. However, there must also be a responsibility on private organizations to be well-informed about the governing rules of privacy and data protection. The expectation that organizations will be well-informed and dutiful in their treatment of personal information builds trust with consumers, while also creating shared standards and expectations

[23] [2017] 1 S.C.R. 751.
[24] *Id.* at para. 2.

about personal information and privacy rights. Several considerations must be made when planning for evolution in the digital marketplace.

International Regulations

The current international efforts in data protection should be considered when identifying key obstacles to strengthening privacy rights and data protection in the Canadian marketplace. The invaluable data gathered from the implementation of the GDPR, including methods of practical enforcement, managing international relations and expected budget requirements, should be utilized when implementing open banking.

Budget

The impact of implementing stricter data protection legislation includes the potential for significant increased costs related to regulation and enforcement. The high cost must be considered when budgeting for privacy and data protection in the evolving digital landscape. Many countries within the E.U. have reported higher costs associated with upgrading regulation infrastructure in preparation for the GDPR. As such, the cost of increased regulation alone must be factored into the Canadian budget.

Penalties

There exists no strict penalty system within Canadian data protection regulations. In order to secure privacy rights in a digital transformation, strict penalties should be imposed to ensure greater compliance by organizations. This is one method to try and achieve balance between innovation and individual rights. The strict penalties imposed by the GDPR act as a caution to global organizations and in turn, strengthens the protection of privacy rights. The imposition of higher penalties makes commercial organizations more likely to respect personal information and ensure the safety of their consumers. Therefore, the penalties imposed by Canadian regulations should be reviewed when considering digital transformation in Canada.

In order for Canadians to feel confident in an open banking system, how should risks related to consumer protection, privacy, cyber security and financial stability be managed?

The strongest protection for individual privacy rights is a combination of clear legislation, well-informed organizations and operational consumer rights and remedies. The implementation of the GDPR has illustrated that global markets need time to educate themselves on data protection changes before they occur, and to adjust to new requirements. Otherwise, a balance between privacy and innovation will not be achievable. For example, the GDPR was proposed in 2012, granted in 2016 and then enforced in 2018, and businesses still weren't ready for the extra requirements[25]. The benefits of providing a large lead up time for organizations to adapt to changes in data protection legislation should be considered to balance competing interests.

Based on the evidence to date, the GDPR appears to be indirectly suppressing free speech, by causing international newspapers to be blocked in the E.U. and acting as a barrier to innovation, by influencing the closure of smaller tech companies with business models that do not comply with the new rules. This information suggests that there is no absolute way to proceed with instituting a digital transformation that fully supports innovation and fully supports the protection of individual privacy rights and personal information.

Initially, there will be some compromise to ensure that a balance is struck between these competing interests. A balance could be achieved by providing several years between advertising new regulations and enforcing said regulations. This time would allow for adequate education of consumers and preparation for compliance by organizations. It is strongly suggested that the Canadian privacy and data protection regulations are amended, and there is a long lead up time between the amendment introduction to enactment.

[25] GDPR Report. *GDPR: the numbers don't lie – the world isn't ready.* 30 January 2018. https://gdpr.report/news/2018/01/30/gdpr-numbers-dont-lie-world-isnt-ready/.

Recommendations

In context of the recent changes that have occurred in the data protection landscape, we suggest that the following recommendations are considered:

1. FIPA recommends that funding is increased for education and awareness campaigns to inform the public about potential risks of open banking and available remedies in case of privacy breaches.
2. FIPA recommends the Canadian government works to implement a proactive reporting culture in organizations and positive treatment of privacy rights that is led by educated individuals.
3. FIPA recommends that the Canadian government works with the Privacy Commissioner and Office of Privacy to develop an accessible complaints process for individuals to report privacy breach concerns.
4. FIPA recommends that the Canadian government increases funding to the Privacy Commissioner and the Office of Privacy. Further, FIPA recommends that the investigative and enforcement powers of the Privacy Commissioner and Office of Privacy are strengthened through legislative amendment, like current data protection and privacy legislation in British Columbia.
5. FIPA recommends that the Canadian government take proactive steps to research and study the impacts that privacy issues in open banking will have on marginalized groups.
6. FIPA recommends that the Canadian government develops a new data protection and privacy framework to comply with open banking and allows enough time for interested groups to provide feedback prior to implementation.

What role and steps are appropriate for the federal government to take in the implementation of open banking?

The cornerstone of individual privacy in the digital economy is informed, meaningful consent. In order to ensure individual rights are protected, the consent of individuals must be thoughtfully obtained by organizations. To gain this balance, there must be clear regulations in place, with clear penalties for breaches. Further, organizations must be committed to conducting better

business practices. Finally, regulators must have the resources to protect individuals if breaches occur. To date, there have been concerns about the methods used on digital platforms by organizations to obtain consumer consent. These methods include presenting lengthy blanket use terms for consumers to agree to and providing insufficient consent forms. These practices need to be monitored to ensure compliance with data protection regulations.

By holding organizations to higher standards when obtaining individual consent, we can potentially decrease the privacy breaches that occur. The mandatory breach laws that came into effect in November 2018 are a positive step forward in putting power back into the individual consumers' hands. However, these new regulations must be balanced by proactive practices that also aim to prevent breaches. Only by having a balanced data protection system, with both proactive and reactive regulations, will individual privacy and consent be respected by organizations.

The potential economic effects of implementing stricter regulations such as the GDPR are significant and may lead to decreased innovation in certain data driven industries. However, these strict regulations are necessary to balance the power between individuals and businesses so that privacy rights are not disregarded. We can continue to monitor the progress of the GDPR to determine the long-time effects of strict data protection regulations. It may prove to be worth the initial decrease in innovation to obtain the security of strict data and privacy protection regulations. This approach is practical, and serves as a reminder that businesses cannot operate freely without limits. These limits are individual rights and protections.