August 10, 2018

The Hon. Dwight Sutherland M.P.
Minister of Small Business, Entrepreneurship and Commerce
Ministry of Small Business, Entrepreneurship and Commerce
Via email: commerce.comments@barbados.gov.bb

Re: Comments on the Data Protection Bill, 2018 on behalf of BIPA, BISSA and ISOC Barbados

These comments are submitted on behalf of the Barbados ICT Professionals Association (BIPA), the Barbados Chapter of the Internet Society (ISOC) and the Barbados Chapter of the Information Systems Security Association (BISSA) (collectively, the "Commenters"). The comments are in response to a request for comment made by the Ministry of Small Business, Entrepreneurship and Commerce.[1]

At this juncture, the comments are preliminary and, should a further opportunity be presented for further submissions to be made, the Commenters reserve the right to reflect any further feedback received from their memberships.

Introduction

The Commenters are grateful for the opportunity created by the Government of Barbados, via the Ministry of Small Business, Entrepreneurship and Commerce for comments to be made on the 2018 Draft of the Data Protection Bill.

At their core, digital economies and information societies generally develop best when the denizen trust the various information service offerings available. The globally accepted wisdom is that the protection of personal data is essential to developing trust in, and adoption of, digital systems such as internet-based commercial website offerings and online government services. The general right to privacy and specifically informational privacy, which this Bill proposes to usher in, is therefore of fundamental importance to the development of Barbados' domestic digital economy. Barbadians will more likely engage and do business with online service providers if they are secure in the belief that they can trust their systems.

Importantly too, businesses faithfully adhering to the obligations of an effective data protection regime will significantly reduce the likelihood of those businesses being the victims of data breaches. In this way, implementing a comprehensive data protection regime will, over time, lessen the negative impact of a data breach on the bottomline of those businesses in Barbados which process personal data. The better the financial health of businesses in Barbados, the better the economy.

It is therefore of critical importance that Barbados gets this foundational pillar of our march towards being an information society, right.

[1] See http://www.commerce.gov.bb/website/index.php/8-news/239-comments-of-the-draft-data-protection-bill-2018

Prevailing Context

Approach

General Observations

1. Lack of inclusion of modern, meaningful privacy-related rights and approaches to data protection

Perhaps the most striking feature of the proposed Data Protection Bill is not the contents, but the elements that are absent. Our appreciation of the requirements for an effective data protection regime in rights-respecting societies has advanced significantly since the Data Protection Bill was originally floated in 2005. It would therefore be valuable to include in the updated 2018 draft, many of the modern concepts which have found favour in modern data protection frameworks such as the European Union's General Data Protection Regulation, the State of California's Consumer Privacy Act of 2018 (AB 375) and, closer to home, the Data Protection acts in international business jurisdictions such Bermuda[5] and the Cayman Islands.[6]

On review, the Bill does not, for example, speak to the right to be forgotten; data portability; privacy by design; breach notification requirements; and the appointment of data protection officers within organisations.

This is not to say, however, that all of these concepts are *necessary* for the establishment of an effective regime. That said, of the matters excluded from the draft, the most significant notions which would add real value are:

(i) Breach notifications

A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to data subjects such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

Accordingly, depending on the nature of the breach and the perceived severity, data controllers and/or data processors should be required to report any breaches of which they become aware within a reasonable period of time to the Data Protection Commissioner and, in certain circumstances, directly to the data subjects also.

The foregoing should, however, be considered against the reality of limited financial resources of smaller businesses in Barbados. Such entities will still be defined as data controllers under the Bill. That said, it is recognised that even small businesses should comply with data breach notification requirements if their core business functions require the significant processing of personal data.

In consideration of the above, it is suggested that the appropriate solution should also limit data breach notification requirements to those data controllers that meet certain criteria:

[5] Personal Information Protection Act 2016, 2016 : 43
[6] The Data Protection Law, 2017 (Law 33 of 2017)

- The data controller operates above a specified financial threshold (for e.g. average annual turnover greater than $500,000/year); or
- The data controller's core functions require them to make significant use of personal data; or
- The data controllers are governmental entities.

(ii) Impact assessments

Impact assessments serve to help data controllers identify any data-related risks prior to implementation. The general idea behind impact assessments is that where the processing of data, especially with newer technologies, is being considered by a data controller and the processing potentially has greater risks for the rights and freedoms of data subjects, a documented impact assessment should be done to assess the likely risks associated with the technology's impact on data protection. In a prevailing context where the Government of Barbados and private sector actors intend to introduce 'smart' technologies and many ventures operating out of the jurisdiction are now taking advantage of blockchain and other cutting-edge technologies, it is important that these parties be required to undertake impact assessments prior to implementation.

(iii) Appointment of data protection officers

In order to ensure effective compliance, an obligation should be inserted requiring the engagement of data protection officers within organisations with the greatest likelihood of causing significant damage to the rights of data subjects in the event of a breach. Specifically, where such organisations process significant amounts of personal data and regularly monitor data subjects. In addition, as a practical measure, this requirement should be limited to public bodies/agencies and private entities whose core-operations require the processing of sensitive information and businesses over a certain turnover threshold (we suggest $500,000.00).

2. No obligations placed on data processors

While often the same party may execute both functions, the roles of data controllers and processors are different. A data controller determines the purposes and means of processing the personal information of a data subject while a processor is responsible for processing the data under instruction from a data controller.

The Bill does not expressly recognise that data processors, through no fault of the data controller, may by their (in)actions, breach the information privacy rights of data subjects. Curiously, however, the Bill does not include any substantive provisions relating to the obligations of data processors. This is a meaningful deficiency in the Bill which will result in data processors escaping liability where, otherwise meaningful data breaches could be attributed to them.

At a minimum, a data processor under the Bill should be separately obligated to:

- maintain a record of all categories of processing activities to demonstrate compliance with their obligations under the Bill;
- implement appropriate technical and organisational measures to ensure the security of any personal data being processed; and
- Notify the data controller of any data breaches in a timely manner.

3. No specific considerations for minors

Children in Barbados are growing up with the internet and other information society services as the norm. It is therefore important that the Bill acknowledges the necessary tension between the reality that persons under 18 years of age are constantly using these data-intensive services with the fact that, depending on their age, they may not be in a position to offer informed consent.

This shortcoming ought to be addressed.

4. Inadequate penalties

Under the current Bill, the highest penalty amounts to BD$100,00.00 (US$50,000.00). By comparison, the maximum fines for breaches of data protection legislation among jurisdictions in the Caribbean that have recently passed legislation are as follows:

- Cayman - US$121,951.00 (BD$243,902.00); Act passed 2017.
- Bermuda - US$250,000.00 (BD$500,000.00); Act passed 2016.
- Saint Kitts and Nevis - US$185,000.00 (BD$370,000.00) Act passed 2018.
- Trinidad and Tobago - up to 10% of a company's annual turnover; Act passed in 2011

Further afield, the approach in the European Union provides for maximum fines of 4% of an entity's turnover, up to a maximum sum of €20 million.

The modern trend is, therefore, towards larger fines to ensure that data controllers and processors are encouraged to implement effective data security mechanisms and dissuaded from infringing the rights of data subjects under the Bill. The current maximum fines are insufficient for this purpose and unless amended upwards, will not likely be sufficiently dissuasive.

5. No definition or parameters in respect of consent

In practical terms, the most common basis for the processing of personal data, including sensitive personal data will be where the data subject has consented. The Bill does not, however, define or provide many parameters outlining the operation of this important concept. At best, the only express consideration in the Bill is the requirement for consent to be in writing.[7]

The Electronic Transactions Act (ETA) provides that electronic records will suffice where the law requires information to be in writing, so long as the information contained in the electronic record is accessible and capable of retention for subsequent reference.

Put another way, when read together with the ETA, the requirements for consent are that:

- consent should be in writing
- consent can be provided via electronic record instead of in writing
- where consent is via an electronic record the record must be accessible
- where consent is via an electronic record the record must be capable of retention for subsequent reference

Even when the provisions of the ETA are read into the Bill, it does not go far enough in delineating how consent ought to operate. For instance, there is no indication of whether the

[7] in sections 6(1)(a) and 7(1)(a) of the Bill which outline the conditions for processing personal data and sensitive personal data respectively

consent must be informed and also no indication of what occurs when a data subject who has consented wishes to withdraw that consent.

To avoid ambiguity and to ensure that consent is validly obtained from data subjects, It is suggested that the Bill be amended to make it plain that:

- consent must be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of his or her personal data.[8]
- a data subject has the right to withdraw consent at any time.
- The data controller holds the burden of demonstrating that a data subject has consented to the processing their personal information.

6. Continuous iteration

Given the rapid rate of advance of information and communication technologies and the new and novel ways in which personal data can be produced, collected and processed, it is envisaged that Parliamentary oversight may be required to update crucial aspects of the data protection regime. It is suggested that the Bill should include a requirement for review by Parliament every 5 years.

7. Self-regulation v external regulation

The Bill speaks to the registration of data controllers. The presumption is that this requirement will serve as part of the regulation/enforcement mechanisms found in the proposed act.

Registration of data controllers is limited in its effectiveness and enforcement of this requirement will, implicitly, depend on how well-resourced the data commissioner will be. In any event, if a data controller simply refuses or fails to register, then the Data Protection Commissioner will not be aware of the operations of that data controller and, ostensibly, the data controller will remain outside of the effective enforceable jurisdiction of the Data Protection Commissioner.

A better alternative approach may be to encourage self-regulation via a combination of impact assessments; the appointment of data protection officers and voluntary notifications.

8. No underlying constitutional right to privacy

The Bill will usher in the concept of informational privacy into Barbados. Informational privacy is an acknowledged subset of a larger right to privacy. Typically, this right is enshrined in the constitution of nation states in the form of a right to respect for private life to serve as a limit on government power and also to affirm its importance to i) human dignity and ii) the enjoyment of the other constitutional rights (freedom of expression; right to property etc).[9]

Curiously, the Bill of Rights contained in the Barbados Constitution does not contain an enforceable right to privacy or data protection. This may prove to be significant with the passage

[8] Consistent with the European Approach under the GDPR at Article 7

[9] See generally, European Union Agency for Fundamental Rights and Council of Europe. 2018. "Handbook on European Data Protection Law, 2018" at p19

of time since there is no constitutional-level right against which the Bill's wide-ranging powers, right-exceptions and requirements may be balanced.

Notably, the Bill bears striking similarity to the contents and structure of the former Malta Data Protection Act[10]. However, since Malta is a member of the European Union, the rights and obligations conferred by the Maltese Act would have been subject to the overriding effect of the EU Charter of Fundamental Rights (EUCFR). The EUCFR confers broad enforceable rights to privacy[11] and data protection.[12]

To ensure that this Bill meaningfully protects the informational privacy rights of Barbadians, its passage should be accompanied by a separate bill amending the Barbados Constitution to include among the enforceable Bill of Rights provisions, a right to respect for private life and a right to protection of private information.

Specific Comments

9. Section 2 - definitions of data controller and data processor

The definition of data controller and data processor, by virtue of their reference to 'person' are unnecessarily vague. At a minimum, these definitions open the proposed act to misguided interpretations that data controller was not expressly intended to include, for example, statutory bodies or Governmental ministries.

Suggestion: re-scope the definition of 'person' in both definitions: to include "a natural or legal person, public authority, agency or other body."

Accordingly, the amended definition of data processor should read

> "a natural (other than an employee of a data controller) or legal person, public authority, agency or other body, who processes personal data on behalf of the data controller"

Similarly, an amended definition of data controller should read:

> "data controller" means
>
> > "(a) any natural or legal person, public authority, agency or other body who alone, jointly or in common with others determine the purposes for which, and the manner in which, any personal data are or are to be processed; or
> >
> > (b) where personal data are processed only for the purpose for which the data are required by or under an enactment to be processed, any natural or legal person, public authority, agency or other body on whom the obligation to process the data is imposed by or under the enactment."

[10] 26 of 2001, Cap 440 of the Laws of Malta. Recently repealed by No 20 of 2018
[11] See Article 7 of Title II thereof
[12] See Article 8 of Title II thereof

10. Section 2 - definition of personal data

The act defines personal data as relating "... to an individual". This definition is unnecessarily broad and without more, could arguably apply to a deceased person's estate for example. The definition should be adjusted to reference living persons. As amended, the first part of the definition of personal data would read:

> ""personal data" means data which relate to a living natural person who can be identified..."

11. Section 2 - definition of sensitive personal data

Under the Bill, sensitive personal data is defined to mean:

> "personal data consisting of information on a data subject's (a) racial or ethnic origin; (b) political opinions; (c) religious beliefs or other beliefs of a similar nature; (d) membership of a political body; (e) physical or mental health or condition; (f) sexual orientation or sexual life; (g) financial record [or position]; (h) criminal record; or (i) proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings."

The essential idea behind sensitive personal data and, by extension, the higher standards associated with its processing is that the context of their processing could result in significant risks to the rights and freedoms of data subjects, such as discrimination.

With this in mind, the current definition is not wide enough and does not cover other data that could readily be used in the Barbadian context to impact a data subject's fundamental rights and freedoms. It is suggested that the definition of sensitive personal data is expanded to also include: genetic or biometric data; membership in trade unions; and nationality.

12. Section 3 - application of the Act

As drafted, section 3 appears to focus the Bill on the actions of data controllers. Further, it limits its scope to situations where, among other things, the data controller is **in** Barbados and also processes data in the context of the controller's business.

Especially when read against the Bill's stated objects and reasons, it is unclear why the drafters have so limited the scope of the Bill to the use of personal data in business contexts. It is also unclear why a broad-based Bill designed to safeguard informational privacy rights would have a singular focus on data controllers.

Further, it is at least arguable that section 3 of the Bill, as framed, results in a statute that places a higher compliance burden on domestic data controllers than it does on their counterparts established outside the jurisdiction who target Barbadians. Simply, Google, Facebook, Twitter, Netflix and LinkedIn don't have to register as data controllers or comply with any of the other substantive requirements of the Bill but they are, ostensibly, still allowed to target Barbadians without the enforcement repercussions or compliance obligations that entities established in Barbados must countenance. This is an undesirable outcome and may serve as tacit encouragement for businesses targeting Barbadians to incorporate outside Barbados.

Suggested solution:

Rewrite section 3 to: i) focus the scope on the processing of personal data of data subjects as opposed to the actions of data controllers; and ii) more clearly define the territorial scope of the Bill.

Per this suggestion, section 3 would read:

> "(i) This Act applies to the processing of personal data in the context of the activities of a data controller or data processor established in Barbados.
> (ii) This Act applies to the processing of personal data of data subjects in Barbados by a data controller or data processor **not** established in Barbados, where the processing activities are related to the offering of goods or services to data subjects in Barbados;
> (iii) For the purposes of subsection (i) each of the following is to be treated as established in Barbados:
>
> > (a) an individual who is ordinarily domiciled in Barbados;
> > (b) a body, association or other entity incorporated, organised, registered or otherwise formed under the laws of Barbados; and
> > (c) any person who does not fall within paragraph (a) or (b) but maintains in Barbados an office, branch or agency through which he carries on any activity related to data processing."

13. Section 4(2)(h) and Section 12 - safeguards for transfers out of Barbados

Section 4(2)(h) establishes as the "eight data principle" underpinning the act that personal data shall not be transferred outside Barbados unless the destination jurisdiction ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of their personal data. "

Section 12(1) then outlines the various factors to be considered in a determination of whether the other jurisdiction's level of protection is adequate and section 12(2) speaks to the exceptions to the eight data principle.

When read in their totality, sections 4(2)(h) and 12 appear to focus primarily on adequacy findings on a government-to-government level. That is: the Barbados government expressly assessing other jurisdictions pursuant to the factors outlined in section 12(1) to determine whether adequate safeguards are in place.

It is suggested that the Bill should also include provisions whereby transfers can be deemed adequate where, in line with the approach adopted in the European Union, the parties to the transfer put in place adequate safeguards which do not necessarily require significant governmental oversight to implement. These safeguards could include:

- Binding corporate rules whereby a data controller in Barbados who is within a group of companies wishes to transfer data to another entity within that group;
- Contractual clauses in the agreements between the Barbados data controller and the entity outside Barbados.

14. Section 12 - adequacy authority

The Bill does not make clear who is responsible for determining whether another jurisdiction possesses adequate safeguards for the lawful transfer of personal data out of Barbados.

Suggested solution: Insert a provision empowering either the Data Protection Commissioner or the relevant minister to prepare a publicly available list of those jurisdictions which are deemed adequate. This provision should include a mandate for the responsible authority to update the list of adequate jurisdictions periodically.

The mooted subsection of section 12 could read:

> "The Minister, after assessing the adequacy of the level of protection using the criteria in subsection (1) may by Order declare that a country, territory or one or more specified sectors within a country, or an international organisation ensures an adequate level of protection within the meaning of subsection (1). The Order shall provide for a mechanism for a periodic review, at least every seven years, which shall take into account all relevant developments in the country, territory or international organisation."

15. Part III - Data Protection Commissioner

Part III of the Bill establishes the office of the Data Protection Commissioner. It is submitted that the provisions in respect of the establishment of the office do not go far enough. The role of Data Protection Commissioner will require the party occupying the role to operate without fear of retribution or discrimination and also to lower opportunities for the officer holder to compromise the integrity of the office. In other words, the Data Protection Commissioner, to be effective, must operate with total objectivity.[13]

Additionally, a cursory review of the functions of the Data Protection Commissioner suggest that in order for the incumbent to have a semblance of effectiveness, significant resources will need to be allocated. This is important since the independence of the Data Protection Commissioner ought to be demonstrated and reflected not just in a notional statement of independence in the Bill, but also in the level of resources allocated to support the Data Protection Commissioner's functions.

In consideration of the foregoing, it is suggested that, at a minimum, the Bill ought to include provisions addressing the following:

- minimum tenure of the office holder;
- The process for appointment of the office holder;
- arrangements for pensions for the Data Privacy Commissioner and her staff;
- Provision of human, technical and financial resources and infrastructure for the effective performance of the role of Data Protection Commissioner;
- Express acknowledgment of the freedom of the Data Protection Commissioner to operate without external directions

[13] This was the very point addressed in ***European Commission v. Federal Republic of Germany***, CJEU, C-518/07

16. Section 14 - drafting error: no subsection (1)

Section 14 does not have a subsection (1), this reference should be removed.

17. Section 14(l) - codes of practice

Section 14(l) when read in its appropriate context, provides that:

"(14) Without prejudice to the generality of subsection (1), the functions of the Commissioner are to… (l) prepare appropriate codes of practice for the guidance of persons processing personal data; "

It is submitted that a more appropriate approach should:

1. make it explicit that any codes to be developed should be of general application to industries/sectors; and
2. require any codes to be developed in consultation with relevant industry/sector associations; interest groups and other relevant stakeholders.

Recommendation: Amend subsection 14(l) to read:

> "(l) prepare appropriate codes of practice for various sectors upon consultation with relevant sector stakeholders for the guidance of persons processing personal data in those sectors"

18. Section 15(2) - payment of fees to request information

Section 15(2) indicates that a data controller is not obliged to provide information to a data subject unless the data subject pays the relevant fees prescribed by the Minister. Without more, no data subject should have to pay fees to access information related to their own personal data.

It is suggested that this section requiring payment of fees is:

a. removed altogether; or
b. replaced with provisions:
    i. limiting payment of fees to repeat requests by the same data subject where the request has already been complied with in good faith by the data controller; or
    ii. limiting any fees paid by data subjects to reasonable charges of the data controller associated with producing the actual personal data requested; as distinct from producing information related to the data. For example, a description of the data being stored/processed and reasons for storing the data should not attract a charge as they would constitute information related to the personal data.

19. Sections 19(4) - undefined court (also applicable to sections 20(2); s21(9); s23, s54, s60)

The Bill refers at sections 19(4); 20(2); 21(9); 23, 54 and 60 to 'court.' The Bill does not, however, define which court it means - Magistrate, High Court or Court of Appeal. This may result in procedural uncertainty where a data subject wishes to proceed to the court for relief. To avoid this uncertainty, the Bill should be amended to expressly define court.

Suggestion: Insert a definition of 'court' into section 2 of the Bill to clarify. The definition could read:

> "Court means the High Court of Barbados, unless the context otherwise requires"

20. Part V - registration of data controllers

In the context of encouraging tech-entrepreneurship and app development, it would be quite onerous if a recent university graduate with a great app idea was required to pay a mandatory fee as a precursor to registration as a data controller. More broadly, in the context of an increasingly data-driven society where an increasing number of businesses provide information-based services which require the processing of personal data, the registration requirements are onerous and may serve as subtle disincentive to entities considering operating from Barbados.

Suggestion: Remove the requirement for registration and focus more on self-regulation whereby data controllers, above a certain threshold are required to appoint data protection officers and self-report.

21. Section 70 - proclamation timing

The Bill in its current form indicates that the proposed act will come into effect "on a date to be fixed by proclamation."

Issue: As currently read, the Bill will likely require data controllers to review their systems with a view to taking corrective measures to ensure compliance with the various requirements to be imposed. This will be a time-intensive and costly exercise which will not likely result in desirable levels of compliance if those impacted by the legislation are not given reasonable lead time.

Solution: An implementation window should be inserted into section 70 in respect of the prosecution of substantive provisions of the Act requiring compliance by data controllers and data processors while the parts concerning the office of Data Commissioner should be given effect upon proclamation. In doing so, this will allow the Data Commissioner to be established and to effect a meaningful awareness campaign leading up to full implementation.

The proposed language could be:

> "(1) This Act comes into operation on a date to be fixed by proclamation.
>
> (2) data controllers and data processors shall take all necessary measures to ensure compliance with the applicable provisions of this Act on or before the expiration of a period of two years from the date of commencement of this Act
>
> (3) no proceedings under this Act may be taken against a data controller or data processor in respect of any data processing done in good faith during the period referred to in subsection (2)"

About the Commenters

BIPA - The Barbados ICT Professionals Association (BIPA) is the island's foremost professional membership organisation for individuals and corporations whose primary focus is the expansion and development of ICT opportunities in Barbados and the Caribbean region. BIPA is dedicated to providing its members with a forum in and through which they can exchange industry information,

network with other members of the ICT sector, undertake advocacy activities on behalf of industry interests, and collaborate with each other to extend the scale and scope of services accessible through the ICT sectors. See: barbadosict.org

ISSA (Barbados) - The Barbados Chapter of the Information Systems Security Association (ISSA) was officially recognised by ISSA in April 2010. As a non-profit organisation, the Barbados Chapter of ISSA is concerned with the promotion of management practices that ensure confidentiality and integrity, while raising national awareness about personal information security and privacy issues. See barbados.issa.org

Internet Society (Barbados Chapter) - The Internet Society (ISOC) is a global non-profit organization founded in 1992 to provide leadership in Internet-related standards, education, access, and policy. The Barbados Chapter of ISOC, a registered not-for-profit, was officially launched on 20 September 2016 and has participated in the work of ISOC by engaging the local Internet stakeholders via key local events including InterCommunity and the Barbados Internet Governance Forum. See isoc.bb

About the Drafter

Prepared under instructions by Bartlett D. Morgan, member of the International Association of Privacy Professionals (IAPP) and Attorney-at-Law at Lex Caribbean. See lexcaribbean.com/attorneys/bartlett-morgan.html