BROADCASTING COMMISSION
PEOPLE▸TRANSITIONING▸DIGITAL

Submission from the Broadcasting Commission on the Data Protection Act, 2017

Introduction: the Digital Economy and Society

1. The world is at an early stage in a 'Fourth Industrial Revolution', which involves the integration of artificial intelligence, robotics, nanotechnology, additive manufacturing, genetic engineering and biotechnology. Artificial intelligence and robotics could replace from 50-90% of all current jobs over the next two or three decades, so it is essential to prepare for this radically different future.

2. A key part of the strategy is to accelerate the transition to a digital society and economy in Jamaica, which involves moving business, commerce, government, education, health care, media and most aspects of personal life online. Adding value to this data requires free expression, wide access, verification, sharing and analysis, which means that life in the digital world will involve the disclosure, collection, storage and monetization of personal data as citizens access news, information, entertainment, education, geo-location/directions, home management and shopping, translations and many other services on and across multiple screens and devices. Platforms will become largely invisible as technologies converge and interoperability becomes the norm.

3. In the digital economy, people must be free to disclose information, but they must also be protected from abuses such as fraud, identity theft and cyber-bullying. Any failure to do so will undermine the development of digital markets in Jamaica. This requires effective policing, but it is at least equally

important to encourage digital literacy so that people can safeguard themselves[1][2].

4. So the goals of content regulation and data protection are fundamentally similar; to enable the transition to a digital society and economy by mitigating abuses and thereby allowing people to have confidence in online interactions and transactions.

5. This common goal is reflected in the mission of the Broadcasting Commission, which is 'to ensure a successful national transition to a digital economy, using the empowering and liberating potential of technological innovation to encourage new forms of business, social, cultural and media development while protecting the people of Jamaica from potential abuses of communication and influence. We guard against malicious, harmful and inappropriate content; we operate public education programs to build the capacity of youth, parents, guardians, teachers and the general public to detect and respond to harmful material; and we work with the media to encourage high standards and trustworthiness in journalism'. We recommend that the new Commissioner adopt a similar approach.

6. We also recommend that the new Commissioner should adopt a similar philosophy of regulation. The regulatory philosophy of the Broadcasting Commission is summarized in the following statement; 'We keep our operations under constant review to ensure that the regulatory framework for Jamaica is as lean, transparent, efficient and effective as possible, with the optimal mix of educational and advisory interventions, legal and economic tools, sanctions and positive incentives'.

7. There is a connection therefore between the goals of data protection and modern content regulation, which is that they are both concerned with

[1] See Office of the Privacy Commissioner of Canada Strategic Privacy Priorities at https://www.priv.gc.ca/en/about-the-opc/opc-strategic-privacy-priorities/the-strategic-privacy-priorities/#economics; and Broadcasting Commission presentation "Connectivity and Monetisation of Personal Information" at International Institute of Communications Annual Conference, 16th October 2016, Bangkok. http://prezi.com/fdpw3aie98lm/?utm_campaign=share&utm_medium=copy

[2] https://www.priv.gc.ca/en/about-the-opc/opc-strategic-privacy-priorities/the-strategic-privacy-priorities/#reputation

protecting against harm and building trust so that citizens can confidently participate in the digital society and economy.

8. Given these overlaps, the Joint Committee may wish to consider the option of combining the two functions of media and internet content regulation in a single agency. This would assist the Government of Jamaica to honor its commitment to the International Monetary Fund to reduce the cost and burden of government, as well as minimizing the number of government agencies with overlapping remits[3].

Governance

9. In order for the Information Commissioner to serve the nation well, it must function at the highest standards of probity and ethical conduct, with the maximum transparency and accountability. It should be a requirement that all decisions of the Information Commissioner be fully documented, explained and justified.

10. There should also be provision for members of the public to complain about the Information Commissioner. The approach in Canada could be considered here. Canada makes provision for the appointment of an Information Commissioner *Ad Hoc* and a Privacy Commissioner *Ad Hoc,* with delegated powers, duties and functions of the Information and Privacy Commissioners in order that he can investigate **Privacy Act** complaints lodged against the Office of the Privacy Commissioner and complaints about the Office of the Information Commissioner, in relation to access requests made to the OIC. This could be a more manageable and efficient administrative arrangement than the establishment and operation of an appeals tribunal.

11. Section 4(3)(b) of the Bill makes provision for the Information Commissioner to perform "such other functions as may be conferred on the Commissioner by the **Access to Information Act**". It is not clear from this provision whether two entities are intended to administer the **ATI Act**, the Information Commissioner and the Access to Information Unit. This should be clarified to avoid both duplication and conflict of functions.

[3] https://www.imf.org/external/np/loi/2017/jam/032917.pdf

Sanctions for breach

12. Criminal Sanctions should be reserved for the most egregious breaches. Some degree of regulatory flexibility (with a gradation of sanctions from mild to severe) is essential in the modern age; cumbersome and excessively punitive regulation is a major deterrent to business development.

13. In the current draft, non-compliance with the provisions of the **Act** is sanctionable as a criminal offence. It is recommended that there should also be the power to impose administrative fines for breaches of the **Act**, similar to the provisions in Article 83 of the **EU General Data Protection Regulation** (EU GDPR).

14. Article 83 of the EU GDPR provides inter alia:

> ***1.*** *… the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation… shall in each individual case be* ***effective, proportionate and dissuasive****.*
>
> ***2.*** *…when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due, regard shall be given to the following:*
>
> *(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;*
>
> *(b) the intentional or negligent character of the infringement;*
>
> *(c) any action taken… to* ***mitigate the damage*** *suffered by data subjects;*
>
> *…*

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

It is recommended that a similar proportionate approach is adopted here.

Ring-fence revenue to develop Digital Literacy

15. It is further recommended that if administrative fines are provided for in the law, it should be a requirement that the part of the proceeds be used to develop digital literacy of Jamaicans. A digitally-literate citizen will be able to recognize when there is an infringement or misuse of her personal information. The Act will not serve its purpose if citizens are not aware of or able to recognize infringements.

Extra-Territorial Application

16. There is an increasing recognition that cyberspace requires rethinking the application of domestic law to businesses as many businesses now operate globally and are not limited by geography or physical presence. The collection, use, and sharing of data occurs among different entities across multiple jurisdictions. In the Business Process Outsourcing (BPO) industry, for example, personal information is routinely transferred across borders.

17. Under section 3(1)(b), the Act applies to foreign entities only if they use equipment in Jamaica to process information. This provision does not provide protection to Jamaican residents against foreign entities that collect personal data but have no physical presence in Jamaica. It is also unclear whether the Act applies to a Data Broker who purchases data for on-selling in a foreign country. This could place local firms at a competitive disadvantage.

18. If the Act does not have extra-territorial effect, consideration could be given to including a provision, such as that in Japan's Act on Protection of Personal

Information (APPI)[4], which places restrictions on the transfer of personal data to foreign countries. The APPI was amended in 2015 to have "extra-territorial effect" on foreign organisations not located in Japan but which provide goods or services to individuals in Japan[5].

19. Similarly, under section 5B (1A) of the Australian **Privacy Act 1988,** non-Australian organisations are bound by the provisions if they have "an Australian link", except where "the act or practice is required by an applicable foreign law". An organisation having an Australian link is defined to include one which "carries on business in Australia"[6].

20. The Canadian law is silent on the issue of extra-territorial effect. However, in 2017, the Federal Court of Canada made an extra-territorial order against a foreign national operating outside of Canada for violating a Canadian citizen's rights under Canada's privacy law (the **Personal Information Protection and Electronic Documents Act** (PIPEDA))[7]. The EU's GDPR also applies extra-territorially.[8]

21. These examples demonstrate the increasing recognition that geographic boundaries have been partly eliminated by the internet, and that this necessitates revision of the principles and approaches to jurisdiction when enacting domestic law.

Consent for Processing Anonymized Data

22. Under section 23 of the **Data Protection Act**, consent must be given for the processing of personal data except in specified circumstances, e.g. when necessary for administration of justice (personal data is defined as data relating to a living individual who can be identified from the data).

23. The experience in Japan is that the requirement for consent proved to be administratively problematic in the context of the increasing use of 'big data'

[4] Law Number: Act No. 57 of May 30, 2003 as amended September 3, 2015
[5] http://www.elexica.com/en/legal-topics/data-protection-and-privacy/11-new-amendments-to-data-protection-law-in-japan
[6] Section 5B(3)(b)
[7] ***A.T. v. Globe24h.com***, 2017 FC 114; see also http://www.barrysookman.com/2017/02/01/pipedas-global-extra-territorial-jurisdiction-a-t-v-globe24h-com/

[8] Article 3 which includes a controller or processor not established in the EU.

analytics and outsourcing. For that reason, the Act on Protection of Personal Information (APPI) was amended to remove the requirement for prior consent to transfer anonymized data, provided specific requirements were followed when disclosing and processing anonymized information. The requirements included a disclosure of the type of items anonymized, the method by which the anonymized data was provided, and the handling anonymized information separately from data with personal identifiers.[9]

24. Consideration could be given to whether a similar treatment of anonymized information should be in the Data Protection Act.

Professor Anthony Clayton, CD, Chairman

Cordel Green, Executive Director

February 27, 2018

[9] http://www.elexica.com/en/legal-topics/data-protection-and-privacy/11-new-amendments-to-data-protection-law-in-japan