Chambers

GLOBAL PRACTICE GUIDES

Definitive global law guides offering comparative analysis from top-ranked lawyers

Data Protection & Privacy

The Bahamas: Law & Practice
Sean McWeeney Jr
Graham Thompson

The Bahamas: Trends & Developments
Sean McWeeney Jr and Christina Justin
Graham Thompson

practiceguides.chambers.com

2021

THE BAHAMAS

Law and Practice

Contributed by:
Sean McWeeney Jr
Graham Thompson see p.14

Contents

1. Basic National Regime

1.1 Laws

Under its Constitution and through various statutes, The Bahamas has developed a legal framework through which the collection, use, handling, privacy and storage of personal data are regulated and protected.

Constitution

Subject to the public interest and the rights and freedoms of others, Article 15 of the Constitution of the Commonwealth of The Bahamas provides citizens a right to protection of the privacy of one's home and "other property", in addition to protection from deprivation of property without compensation. Similarly, Article 21 of the Constitution addresses the privacy of "other property" and further provides that no person should be subjected to a search of their person or property except with their consent, unless such search is reasonably justifiable or executed to protect the rights and freedoms of other persons. These constitutional provisions confer protection in respect of unlawfully obtained personal information and data by way of a data breach, at least where the offending party is the state or a person exercising public powers or functions. Obtaining personal data from an individual's computer, phone or other electronic device could very well constitute a breach of a fundamental constitutional right unless it can be justified by reference to one of the prescribed exceptions under the Constitution.

Data Protection (Privacy of Personal Information) Act

The Data Protection (Privacy of Personal Information) Act, 2003 (DPA) is the principal law governing the collection, processing, retention, use and disclosure of personal data, and is broadly based on the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980). DPA focuses on the core principles of data collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and data controller accountability. Its key definitions, concepts and principles are described in some detail below.

Data Controller, Data Processor and Data Subject

Under DPA, a "data controller" is defined as a person that determines the purpose and manner in which personal data is to be processed (whether alone or in conjunction with others). This role is to be contrasted with that of a "data processor", who processes personal data on the data controller's behalf. Notably, a "data subject" is defined as a (living) individual who is the subject of personal data.

Personal Data and Sensitive Personal Data

DPA makes a clear distinction between "personal data" and "sensitive personal data". Personal data refers to data relating to a living individual who can be identified from the data alone or from the data when considered together with other information that is in the possession of the data controller.

"Sensitive personal data" under DPA refers to personal data as it relates to the following:

- racial origin;
- political opinions;
- religious or other beliefs;
- physical or mental health (subject to certain exceptions);
- trade union involvement or activities;
- sexual life;
- criminal convictions;
- the commission (or alleged commission) of any offence; and
- any proceedings for any offence committed, and the disposal of such proceedings or any sentence made by any court during the course of such proceedings.

Sensitive personal data is given a lengthy definition in the "Interpretation" section of DPA, but it is seldom mentioned in the statute. Section 30(1)(a) of DPA gives the Minister responsible (currently the Minister of Finance) the authority to make regulations providing for additional safeguards relating to sensitive personal data. However, no such regulations have yet been promulgated. Consequently, sensitive personal data does not possess greater legal weight, nor require any safeguards over and above those that apply to regular personal data. Notably, genetic data, biometric data and sexual orientation data (not to be confused with sexual life data) are excluded from the classification of personal data under DPA.

Data Subject Consent

The notion of data subject consent plays an important role under DPA. One example of this is a data subject's ability (or that of someone acting on their behalf) to waive any restriction or exception to the disclosure of personal data via their request or consent (Section 13(h) of DPA). Similarly, the transfer of personal data outside The Bahamas may be made upon the express or implied consent of a data subject (Section 17(8) of DPA). It follows that where a data subject has made a request pursuant to their right of access under DPA that would involve disclosing personal data relating to another data subject, the data controller is not obliged to disclose such data unless the other data subject has consented to the same as well (Section 8(5) of DPA).

Territorial Scope

Unlike the extraterritorial nature of the EU's General Data Protection Regulation (GDPR) or Brazil's recently enacted *Lei Geral de Proteção de Dados* (LGPD), DPA in The Bahamas has only limited extraterritorial effect (as it concerns data controllers). Under Section 4(1) of DPA, the Act only applies to:

- data controllers established in The Bahamas (where the data is processed in the context of the local establishment); and
- data controllers established outside The Bahamas that use equipment in The Bahamas for processing data (other than for transit through The Bahamas).

In the above context, an "established" data controller can be any of the following (in accordance with Section 4(3) of DPA):

- an individual ordinarily resident in The Bahamas;
- a body incorporated or registered under Bahamian law;
- a partnership or other unincorporated association formed under Bahamian law; and
- any person that does not fall into any of the foregoing categories but maintains an office, branch or agency in The Bahamas through which they carry on a business activity or regular practice.

It can be seen, therefore, that a nexus to The Bahamas of the kind described above must be established in order for DPA to apply outside the jurisdiction.

Core Data Controller Obligations

Data controllers owe a statutory duty of care to data subjects in relation to the collection of personal data (or information intended for inclusion in such data or in dealing with such data), pursuant to Section 12 of DPA.

The core duties imposed on data controllers in connection with any personal data kept by them and in accordance with DPA are as follows:

- to collect data using means which are lawful and fair in the circumstances of the case;
- to ensure the collected data is accurate (and kept up to date where necessary);
- to only keep data for one or more specified and lawful purposes;
- not to disclose or use data in a manner that is incompatible with the aforementioned purpose(s);
- to ensure data collected is adequate, relevant and not excessive in relation to the aforementioned purpose(s);
- not to keep data for a period longer than necessary for the aforementioned purpose(s) (except where the data is kept for historical, statistical or research purposes); and
- to take appropriate security measures to prevent unauthorised access to data and to prevent the alteration, disclosure or destruction of data, and to guard against the accidental loss or destruction of data.

Data Breach Notifications

It should also be noted that DPA places no positive duty on data controllers or data processors to notify data subjects of a data breach incident affecting their personal data. Thus, where such a data breach occurs, data controllers are faced with the option to either not inform the data subject of the breach, or, in the spirit of good corporate governance, transparency and "best practices", to disclose to the data subject that a breach has occurred and/or seek guidance from the Data Protection Commissioner (DPC).

Enforcement and Penalties

The enforcement of DPA is the statutory responsibility of the DPC. In accordance with Part III and Part IV of DPA, the DPC has the authority to, inter alia:

- investigate (or cause to be investigated) claims involving suspected violations of DPA;
- issue an enforcement notice to a data controller or processor requiring a data controller to rectify or erase data subject to an investigation;
- issue an enforcement notice requiring the production of evidence or compliance as it relates to an investigation;
- issue a prohibition notice (as it relates to international data transfers) prohibiting such transfer absolutely or until a specified step is taken with a view to protecting the interests of the data subject(s) concerned;
- issue an information notice requiring a person to furnish information in connection with a matter specified in the same;
- request an authorised officer to inspect, examine, operate and/or test any data equipment located on the premises of a data controller or data processor after having given evidence on oath to a Magistrate to request that such a search be carried out in furtherance of an investigation; and
- institute summary proceedings for an offence committed under DPA.

Penalties for persons found guilty of offences under DPA are prescribed as follows:

- on summary conviction (before a magistrate): a fine not exceeding BSD2,000; or
- on conviction on information (in the Bahamas Supreme Court): a fine not exceeding BSD100,000.

Upon the conviction of an offence under DPA, the court may also order that any data associated with the commission of the relevant offence be forfeited, destroyed or erased (as per Section 29(2) of DPA).

Other Relevant Laws and Regulations

Outside of sector-specific regulations, the following enactments are particularly noteworthy.

The Electronic Communications and Transactions Act 2003 (ECTA) brought about the legal recognition of electronic communications, electronic contracts, electronic signatures and electronic information as they relate to commercial and other business transactions. ECTA also provides a definition of "electronic authentication" in connection with the verification of the originator of electronic communications and for the purpose of ensuring that nothing has been altered during transmission. Of similar importance is Section 11 of ECTA, which addresses the retention of electronic communications. Where electronic documents are required to be retained by law, it is critical that they remain:

- accessible;
- usable for subsequent reference;
- in the same or similar format in which they were generated, sent or received; and
- retained in a way that enables identification of their origin and destination, including information showing the date and time they were sent.

The Computer Misuse Act 2003 (CMA) provides for the protection and securing of computer material(s) against unauthorised access or modification, as well as providing definitions of frequently used terms such as "decryption information" and "encrypted data". Part II of CMA deems the following to be an offence:

- unauthorised access to computer material;
- access to computer material with intent to commit or facilitate the commission of an offence;
- unauthorised modification of computer material;
- unauthorised use or interception of a computer service;
- unauthorised obstruction of use of a computer; and
- unauthorised disclosure of an access code (password).

Notably, CMA has extraterritorial effect pursuant to Section 11 where it is provided that, in relation to any person, despite their nationality or citizenship and irrespective of whether they are currently physically located in or outside the jurisdiction of The Bahamas, the provisions of CMA nonetheless have effect so long as:

- the accused is alleged to have committed the offence while physically located in The Bahamas at the material time; or
- the relevant computer, program or data was in The Bahamas at the material time.

Furthermore, Section 11(3) of CMA provides that even where an offence under CMA has been committed in a place outside The Bahamas, it may be dealt with as if the offence had been committed within the jurisdiction of The Bahamas, provided, of course, that the other predicates for the offence are established as well.

1.2 Regulators

See **1.1 Laws**.

As noted above, the DPC – through the Office of the Data Protection Commissioner (ODPC) (a corporation sole) – is responsible for the day-to-day enforcement of the provisions of DPA. However, the ultimate, overarching regulator is whichever Minister of the government is assigned data protection as part of their ministerial portfolio. Presently, the Minister responsible for data protection is the Minister of Finance. Section 30 of DPA gives the Minister the authority to make regulations for a number of purposes, including:

- providing for additional safeguards in relation to sensitive personal data;
- prescribing additional circumstances in which a prohibition, restriction or authorisation should be made for the further protection of the interests of data subjects;
- prescribing fees in connection with matters arising under DPA; and
- prescribing further offences and penalties for non-compliance.

Initiation of Investigations

The DPC may launch an investigation into whether a data controller or data processor has contravened any provision of DPA either via a complaint in writing by a data subject or based on its own considered opinion (pursuant to Section 15 of DPA). Once a complaint is received by the DPC, a determination will be made as to whether the complaint is frivolous or vexatious before notifying the individual who lodged the complaint whether the investigation will be carried out.

Where the DPC is of the opinion that a data controller or data processor has breached or is breaching a provision of DPA, it has the authority to serve an enforcement notice on the data controller or data processor, requiring them to take a specified step (as detailed in the notice) within a specified time. An enforcement notice may also require the data controller or data processor to rectify or erase any data concerned or to supplement the data, as the case may be, in accordance with Section 15 of DPA.

1.3 Administration and Enforcement Process

As mentioned previously, the DPC is tasked with investigating complaints and enforcing the provisions of DPA. There are a number of offences laid down in DPA, pursuant to Section 29 of which persons found guilty of any offence referred to therein will be subject to a penalty (see **1.1 Laws** (Enforcement and Penalties)).

Investigation and Imposition of Penalties

ODPC has made available on its official website a Policy Statement and Guidance on Complaint Handling (2012) (the DPC Complaints Handling Policy), which is non-binding from a legal standpoint but is certainly persuasive in terms of guidance as to best practices. In accordance with Part II of the DPC Complaints Handling Policy, it is first suggested that a data subject should lodge a complaint with the data controller (preferably to senior management of the relevant company) in an effort to resolve the matter amicably as early as possible (though they can, if they prefer, make a direct complaint to ODPC instead). Where the data controller has either not complied with the request (or ignored it) or the data subject is not satisfied with the way in which the request or complaint was handled, it is then suggested that the data subject contacts the DPC for further assistance.

Essentially, data subjects may make complaints via a written request, called a Data Protection (Privacy) Complaint Form (Complaint Form), to the DPC. Complaints may also be made verbally via telephone where the data subject making the complaint is unable to submit the Complaint Form. The form is available for use on the ODPC website and should be accompanied by written documentation as evidence to support any claim or allegation made as it relates to the data subject's concern or complaint. A Complaint Form may be completed through a representative or agent if the data subject does not wish to complete the form themselves. The Complaint Form asks the data subject or their agent whether any of the following has occurred:

- an institution has inappropriately collected personal information pertaining to the data subject;
- an institution has inappropriately disclosed personal information pertaining to the data subject;
- an institution has inappropriately deployed personal information pertaining to the data subject;
- an institution has inappropriately disposed of personal information pertaining to the data subject; or
- "other" (this category is provided in case a complaint does not neatly fit into any of the foregoing categories).

The Complaint Form also asks the data subject for details of the complaint and a description of how they would like the privacy complaint to be resolved. Once submitted, ODPC should acknowledge receipt of the Complaint Form within three working days (provided it is a valid complaint) and the alleged offending data controller or processor will, after being notified of the nature of the complaint, have 21 days to respond to the DPC. It should be noted that complaints are treated with strict confidence, though there may be instances where the DPC will need to disclose the contents of the complaint to the relevant institution (with the data subject's consent). Consent to disclose details of the complaint to the relevant institution is also asked for in the Complaint Form.

The DPC will make its best efforts to contact the relevant institution with a view to meeting with them (mainly to establish facts) and finding the best solution given the circumstances. In any event, the DPC will review the response of the institution and feed back the results of the investigation to the data subject. Any action that should be taken or that is proposed would also be communicated to the data subject at this time (as per Section 5.4 of the DPC Complaints Handling Policy).

Respondent's Due Process and Appeals Rights

As previously described in **1.1 Laws**, after the completion of an investigation, the DPC has the ability to issue an enforcement notice, information notice or prohibition notice – depending on the context. Dissatisfied institutions have a right to appeal. Section 24 of DPA states that appeals may be made to – and determined by – the court, in respect of a requirement imposed under an enforcement or information notice or a prohibition outlined in a prohibition notice. The appeal must be brought within 21 days of the date of service of the relevant notice.

1.4 Multilateral and Subnational Issues

See **1.6 System Characteristics**.

1.5 Major NGOs and Self-Regulatory Organisations

There are no major privacy or data protection non-governmental organisations (NGOs) or industry self-regulatory organisations (SROs) connected specifically to data protection. Over the years, there have been various civil rights and accountability/transparency groups that have spoken out – and in some instances litigated on a "judicial review" basis – concerning a few select data privacy and data protection issues (which shall be explored later in this guide), but only insofar as they concern the general governance of the country and/or the (lack) of freedom of information surrounding various government policies, new legislation, or the grant of licences or governmental approvals for controversial development projects.

1.6 System Characteristics

There are some perceived similarities between Bahamian data protection law and that of other jurisdictions. As was explained

in **1.1 Laws**, DPA dates back to 2003 and is modelled on the OECD Privacy Guidelines of 1980. Consequently, the Act does not cover many of the contemporary privacy issues covered in more recent comprehensive legislation and regulation coming out of jurisdictions like the EU, Brazil or some states within the United States.

The Bahamian data protection framework is not aggressively enforced, as is the case in many other jurisdictions in the "developed world". ODPC remains relatively quiet on privacy issues of national concern and does not regularly update its website; in fact, it has not posted any additional guidance for the public or data controllers on its website since 2013. Furthermore, although no regulations or codes of practice have been developed under DPA since its enactment, DPA does cover the most fundamental protections for data subjects adumbrated in the OECD Privacy Guidelines.

As alluded to previously in **1.1 Laws**, DPA and the GDPR share similar definitions for personal data, sensitive personal data, data controller and data processor, though the GDPR expands on the classification of certain types of data to include such identifiers as biometric data, sexual orientation, genetic data, location data and philosophical beliefs. Similarly, DPA, like the GDPR, covers core data privacy principles such as lawfulness, fairness, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality.

However, steps taken to ensure that data controllers are abiding by these principles and the associated accountability standards are much more detailed under the GDPR. One example of this is the lack of a data breach notification requirement under DPA, whereas under the GDPR data controllers are obliged to inform data subjects of such a breach within 72 hours. Another example is the requirement under the GDPR for data controllers to appoint a Data Protection Officer (DPO) to act as the contact point for data subjects and the data protection authority; this is not a requirement under DPA. It has been suggested, however, through non-legally binding guidance from ODPC that there should be a contact person within an organisation to handle data subject access requests (DSARs).

1.7 Key Developments

Unsurprisingly, most of the developments in data privacy law in The Bahamas over the last 12 months have been closely associated with the implementation of the Emergency Powers (COVID-19 Pandemic) Regulations and Orders (and the various rules and legislation stemming therefrom) enacted as a result of the COVID-19 pandemic. During the early stages of the COVID-19 outbreak in The Bahamas, in common with most other countries, emergency laws were put in place. These included COVID-19 screening requirements involving the mandatory disclosure of personal health and travel history information, and the provision of biological samples to health officers with a view to assessing the relevant person's health. In addition, persons were subjected to mandatory electronic monitoring through an installed contact tracing mobile phone app upon arrival in the jurisdiction (after travel).

Another key development was the enactment of the Property (Execution of Deeds and Documents) Act 2020, Section 3 of which now allows electronic signatures to be electronically attached to deeds. Deeds may take the form of an electronic communication as per Section 2 of ECTA, and an electronic signature (in accordance with Section 9 of ECTA) used as a method of execution on the deed will be considered valid unless a contrary intention is proved. Prior to this, deeds were not permitted to be executed electronically, although a wide range of other documents were capable of electronic execution under earlier iterations of the legislation.

Also, legislation in the last two years has imposed new data disclosure requirements on companies and other entities (and their owners or controllers) with a view to bringing The Bahamas into greater conformity with the EU, OECD and/or FATF reporting regimes concerning AML and KYC. The legislation dealing with registers of beneficial ownership and commercial entities reporting are emblematic of this particular trend, adherence to which is vital to avoid EU blacklisting.

1.8 Significant Pending Changes, Hot Topics and Issues

Expected Updates to Legislation

There are some significant changes expected in relation to privacy legislation. It was recently announced that the government of The Bahamas (in partnership with the International Telecommunications Union and the Inter-American Development Bank) intends to launch a National Cybersecurity Project with a view to implementing a national security strategy and establishing a Computer Security Incident Response Team. This is an effort to increase cybersecurity in general within the jurisdiction (particularly in relation to government agencies) and to boost The Bahamas' ranking on the UN Global Cybersecurity Index as the government presses forward with its goal of digital transformation of e-government services. It is expected that the trio of cyberlaws enacted in 2003 (DPA, CMA, ECTA) will finally see updates in the near future in furtherance of this objective.

Cyber-attacks

Since the onset of the COVID-19 pandemic, there has been an observed spike in cyber-attacks in both the public and private sectors. There have been reports of cyber-incidents involving schools as they have tried to navigate the transition to virtual learning on various online platforms. Similarly, there was a par-

ticularly notable (and controversial) cyber-incident involving a public hospital where confidential patient records were leaked on social media, including the names and addresses of patients who were receiving HIV/AIDS treatment.

The digital database of the Registrar General's Department also experienced a hack and resulting leak of Companies Registry information that, although not confidential, normally requires a fee to view.

Vaccines

It will be most interesting to see how the COVID-19 vaccine rollout is received by the Bahamian public, many of whom are sceptical of receiving the vaccine for a variety of reasons. It has recently been reported that the Bahamian government is exploring the option of issuing vaccine passports to facilitate travel. This may raise some privacy concerns as some may feel pressured to receive the vaccine (which will not be mandatory) in order to travel or access certain services. There are also concerns over how data in connection with the same will be managed and shared amongst interconnected institutions.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

Data Protection Officers

DPA does not require the appointment of a DPO. Under the (non-binding) Guide for Data Controllers (GDC) provided by ODPC, there is a recommendation that staff of institutions that are deemed data controllers under DPA should receive appropriate training, and that an internal data protection policy should be put in place to ensure compliance with the law (in accordance with Section 8 of DPA where necessary measures should be put in place to facilitate a DSAR). Elsewhere, the DPC Complaints Handling Policy states that a "contact person" should be appointed to handle complaints, though here again this is not required by statute. Some local institutions have appointed DPOs as a matter of best practice.

Authorisation of Data Collection, Use and Other Processing

Interestingly, DPA does not state (in a singular section) the grounds upon which the collection, use and processing of personal data may be authorised. However, Section 1 of GDC, which is non-binding, provides that processing personal data must be necessary for (generally), inter alia:

- preventing injury or damage to the health of the data subject;
- preventing serious loss or damage to the property of the data subject;
- protecting the vital interests of the data subject if seeking consent is likely to damage those interests;
- the administration of justice;
- the performance of a function conferred on a person by or under an enactment; and
- the purpose of legitimate interests pursued by a data controller (except where processing is unwarranted).

Privacy By Design

DPA does not expressly require software or app developers to integrate a privacy by design framework, approach or strategy in the implementation of IT systems or the creation of software, apps or electronic services. Some core principles of privacy by design, including transparency, preventative measures, visibility and security, are addressed in Section 13(1) of the Payment Instruments (Oversight) Regulations 2017 (PIOR), which states that payment service providers should implement measures to address consumer protection, education and privacy. Section 13(2) of PIOR further states that payment service providers should adopt policies on, inter alia, safe operations, privacy of customer information and transparency of products and services.

Privacy Impact Assessment

There is no requirement to conduct a Privacy Impact Assessment (or Analysis) under DPA. It should be noted, however, that under the Bahamian financial services legislative framework there are instances where risk assessments must be carried out – typically to prevent and mitigate risks associated with money laundering and the financing of terrorism and terrorist organisations. An example of this requirement can be found in the recently enacted Digital Assets and Registered Exchanges Act 2020 (DARE), which necessitates a risk assessment to be carried out, as well as the implementation and maintenance of policies and procedures to ensure compliance with the Proceeds of Crime Act 2018 (POCA), the Anti-Terrorism Act 2018 (ATA) and the Financial Transactions Reporting Act 2018 (FTRA), in connection with digital asset business service providers. Furthermore, any guidelines or policies published by the Securities Commission of The Bahamas (SCB) as they relate to risk management must also be followed (as per Section 26 of DARE).

Adoption of Internal or External Privacy Policies

See **2.1 Omnibus Laws and General Requirements** (Privacy By Design).

DPA does not require data controllers to have internal and external privacy policies in place, although this is encouraged by DPC under GDC and the non-binding DPC Checklist for Handling Personal Information (DPC Checklist). The DPC Checklist, which was adopted from the Privacy Commission of Canada, states that such policies and procedures will help staff

know how to handle DSARs or requests for personal information from government bodies, non-governmental organisations, individuals or the media. Section 7 of GDC further provides that a minimum standard of security includes taking reasonable measures to ensure staff are made aware of the organisation's security measures in furtherance of the data controller's core duty under Section 6 of DPA to have in place appropriate security measures to prevent unauthorised access to data. It is implied that privacy policies would fulfil this criterion (but this is not legally mandated).

Data Subject Rights

Under DPA, data subjects are entitled to a right of access (subject to some exceptions) to their data, a right of rectification or erasure of their personal data, and a right to prohibit the use of their data for purposes of direct marketing.

A data subject may make a (written) DSAR to the relevant data controller with respect to accessing their data. Where the request is valid and does not contravene the provisions of DPA, the data controller will have 40 days to provide a response and either:

- inform the data subject of the data kept by them – inclusive of any personal data;
- supply the data subject with a copy of the information associated with the data; or
- provide an explanation of the data where said data may be unintelligible or otherwise expressed in terms that are not easily understood by the data subject (as per Section 8(1) of DPA).

Under Sections 10 and 11 of DPA, data subjects may also make a written request to a data controller pursuant to their right of rectification or erasure of data and their right to prohibit the processing of their data for the purposes of direct marketing where one of the core data controller obligations has been contravened under Section 6 of DPA.

Where a data controller refuses a DSAR in accordance with DPA, they should do so in writing, explaining why the request is being refused (for example, the request is vexatious, the data is confidential or otherwise cannot be provided as it falls under an exception provided under DPA) and indicate to the data subject that a complaint can be made to the DPC thereafter in connection with the refusal.

DPA does not specifically address data portability. Data subjects that object to the collection, use or transfer of their data on the ground that their data has been collected, used or transferred in contravention of a DPA provision should write to the relevant data controller in the first instance in connection with the complaint and then to the DPC (either individually or through an agent) if they are not satisfied with the response (see **1.3 Administration and Enforcement Process** (Investigation and Imposition of Penalties) for more details on this process).

Anonymisation, De-identification and Pseudonymisation

Data that has been anonymised or de-identified would not be caught under the definition of personal data under DPA. Under DPA, personal data relates only to living individuals that can be identified from data directly, or from data in conjunction with other information possessed by the data controller.

Profiling, Automated Decision-Making, Online Monitoring, Big Data Analysis, Artificial Intelligence and Algorithms

There are no specific restrictions, allowances, regulations or guidelines relating to "big data" analysis, artificial intelligence (AI), algorithms or online monitoring under Bahamian law.

ODPC has released (non-binding) guidance notes with respect to data protection and political parties (DPC Political Campaign Guidance). These notes briefly address profiling and automated-decision making. Profiling is not expressly forbidden under DPA, although obtaining data for the purposes of direct marketing through deceptive or unlawful means may be considered a contravention of DPA. The DPC Political Campaign Guidance reiterates the "absolute" right for a data subject to prohibit the processing of personal data for the purpose of direct marketing while reaffirming (per Section 4) that political parties should be careful when conducting market research communications with citizens. Recording attitudes based on responses to such research communications in a way that does not personally identify the individual is of supreme importance. It is thus implied that, where personally identifiable information does need to be recorded and the individual is consequently profiled (with a view to predicting voting behaviour based on responses to surveys and tailored communications or promotional materials based upon attitudes to various social issues, for example), then any future communication should be prefaced by stating that their information is being collected for the purposes of marketing and respondents have the right to opt out of proceeding any further. In such cases, automated-decision making, profiling and direct marketing are inextricably linked.

Lastly, under (non-binding) GDC, the DPC suggests that data subjects are, subject to exceptions, entitled to know the logic involved in automated decisions. Note that this is not explicitly referred to in the corresponding section in DPA (Section 8). Under GDC, however, data controllers are told that such information is encompassed under the criteria of information that should be provided to a data subject pursuant to a data subject's right of access (unless they are exempted under DPA).

"Injury" and "Harm" in the Context of Bahamian Data Protection Law

Under DPA, any restrictions or exceptions to the disclosure of personal data will not apply where such disclosure is urgently required in order to prevent injury or other damage to the health of a person or serious loss of or damage to property (Section 13(d) of DPA). Similarly, as previously mentioned, the DPC may prohibit an international transfer of data where such a transfer would likely cause damage or distress to any person (Section 17(2) of DPA). It is not made clear as to whether the "health of a person" (in the context of disclosure) also extends to a data subject's mental health, but it is submitted that the better view is that it does.

2.2 Sectoral and Special Issues

Financial Data

Interestingly, banking and financial data is not considered sensitive personal data under DPA. This may partly be due to the fact that The Bahamas has an extensive, highly developed and heavily regulated financial services legislative framework. The handling, use, retention and confidentiality of banking information is largely addressed under that framework, particularly in the Banks and Trust Companies Regulations Act 2020. Nevertheless, any personally identifiable information collected by a banking institution would still be subject to the provisions of DPA, unless otherwise exempted.

Health Data

Health (inclusive of "physical" and "mental" health) data is considered sensitive personal data under DPA. By extension, this may also include "sexual life", which should also be treated as sensitive personal data. It does not include data kept by an institution (data controllers) in relation to the physical or mental health of its employees in the ordinary course of personnel administration (as per Section 2(1) of DPA). Furthermore, medical practitioners have a statutory obligation not to act in a way that is contrary to medical ethics, including any wilful or reckless betrayal of professional confidence under the Medical Act 2014.

Communications, Voice Telephony, Text Messaging and Electronic Communications Data

Communications data (inclusive of voice telephony, text messaging and electronic communications) is not categorised as sensitive personal data under DPA per se. A communication will be distinguished as sensitive personal data where it can be related or traced back to an identified living individual and the contents of that communication refer to an individual's race, political opinions, religious or "other" beliefs, physical or mental health, trade union involvement or activity, sexual life or criminal past (or allegations).

"Communications data" is defined under the Interception of Communications Act 2018 (ICA) as, inter alia, any traffic data comprised in or attached to a communication (for the purposes of any postal service or communications network) via a "transmitted communication". It is important to note that communications data does not include the actual contents of a communication. A "communication" under ICA includes anything comprising speech, music, sounds, visual images, or data of any description (which, in most circumstances, can lead to the identity of an individual being discovered).

Children's or Student Data

Children and students do not enjoy special privileges under DPA as the Act does not distinguish between children and adults. Privacy as it relates to student records would fall under personal data under DPA, although data collected in connection with any of the subcategories of sensitive personal data will be deemed sensitive for the purposes of DPA.

Employment Data

Employment data is not specifically mentioned under DPA and therefore is not categorised as sensitive personal data insofar as that data does not include – or is not inextricably linked to – some statutory sensitive personal data category.

Union Membership, Sexual Orientation, Political or Philosophical Beliefs

See **1.1 Laws**.

Internet, Streaming and Video Issues

Browsing data, viewing data, cookies, beacons, location data, tracking technology, etc

Browsing data, viewing data, cookies, beacons and location data (other than tracking technologies that have been authorised to be used through surveillance legislation) are not regulated under the provisions of DPA and would only be classified as sensitive personal data where such data can be used to identify an individual. Pursuant to guidance provided by the DPC, internal and external privacy policies are encouraged in order to explain to the end user what kind of data is being collected from them during the browsing experience. It is also best practice to have a cookies policy in place with a view to being transparent about how any collected data will be used.

Social media, search engines, large online platforms

Where such online platforms meet the criteria of applicability of DPA, they will be treated as businesses or online intermediaries under ECTA (and therefore ultimately as data controllers – though in some instances with fewer liability risks) and be subject to Bahamian data protection and e-commerce law. There is no specific privacy or data protection policy relating to

the regulation of social media, search engines and large online platforms.

Addressing hate speech, disinformation, etc

Hate speech and disinformation campaigns became a hot-button issue at the onset of COVID-19 in The Bahamas, with many fake news items being shared on social media. This led to the government briefly imposing an emergency law banning the publication of "fake news" calculated to incite public panic, fear or hatred. This provision quickly fell away. Under the Penal Code, the offence of criminal libel is also available as an avenue of recourse for victims of online abuse. Similarly, the remedy of civil action for defamation is available as well.

It should be further noted that DPA does not recognise any "right to be forgotten", right to data portability or rights to object to the sale of data as is afforded under the GDPR and in other jurisdictions.

2.3 Online Marketing

Unsolicited Commercial or Marketing Communications

Data subjects have the right to prohibit processing for purposes of direct marketing under DPA, and may opt out of such via a written request. Internet or online marketing is not heavily regulated in the jurisdiction outside of DPA (unlike broadcasting networks, as explained below).

As it relates to telemarketing calls and texts, the Communications Act 2009 (CA 2009) provides that the Utilities Regulation & Competition Authority (URCA) may prohibit the use of a network or carriage service to provide unsolicited communications in order to reduce or eliminate annoyance, inconvenience or anxiety, pursuant to Section 47 of CA 2009.

The non-binding guidance provided by the DPC in connection with data protection during political campaigns is instructive (see **2.1 Omnibus Laws and General Requirements**).

2.4 Workplace Privacy

Workplace privacy or surveillance is not directly addressed under the Employment Act, although it is an offence under CMA to access someone's computer (or other device) without their knowledge or consent. Employers may ask their employees to waive privacy rights as they relate to company property or software (eg, computers, smartphones, etc) via an employment contract with a view to monitoring, for example, online behaviour while using company property.

2.5 Enforcement and Litigation

From an enforcement and litigation standpoint, the case law in The Bahamas as it relates to data protection violations is scant. There is nothing precluding a data subject from filing a lawsuit against a data controller for an alleged contravention of DPA where there is an alleged breach of the statutory duty of care owed to data subjects and the obligation to utilise appropriate safeguards to protect personal data from unauthorised access. Class action suits are permissible in the jurisdiction but they are seldom used.

There have been no major reported cases centring around the provisions of DPA.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

There are laws and standards that are applicable to law enforcement agencies with a view to accessing data for serious crimes.

Section 88 of CA 2009 provides that, as a matter of national interest, licensees under the Act must ensure that their networks enable the ability to hear, listen and record private conversations in accordance with and pursuant to authorisation granted under the Listening Devices Act (now repealed and replaced by ICA). Note that DPA does not apply to personal data kept with a view to safeguarding the security of The Bahamas in the opinion of the Minister or the Minister of National Security, nor will any restriction or exception to the disclosure of personal data apply where such disclosure is required for the investigation of an offence or by any enactment or Court order.

Pursuant to ICA (an Act that was met with some public controversy), communications can be intercepted in accordance with an interception warrant, which can be granted by a judge upon application (Section 5 of ICA). Obtaining information under these provisions must be shown to be necessary in order to prevent or detect a specified offence where there are reasonable grounds to believe such has been committed or is about to be committed, or where the information is required under a mutual legal assistance agreement between the government of The Bahamas and some foreign government. Such an application is made by the Attorney General.

3.2 Laws and Standards for Access to Data for National Security Purposes

See **3.1 Laws and Standards for Access to Data for Serious Crimes**.

3.3 Invoking Foreign Government Obligations

See **4.6 Limitations and Considerations**.

As far as is known, The Bahamas does not participate in a Cloud Act agreement with the United States.

3.4 Key Privacy Issues, Conflicts and Public Debates

See **1.8 Significant Pending Changes, Hot Topics and Issues**.

4. International Considerations

4.1 Restrictions on International Data Issues

Generally, there are only limited restrictions on international data transfers of personal information. Section 12(2) of DPA provides that a data controller must use contractual or other legal means to provide a comparable level of protection from any third party to whom it discloses information for the purposes of data processing. A third party in that instance is often a cloud service provider. Furthermore, under Section 17 of DPA, the DPC possesses the ability to prohibit the transfer of personal data outside The Bahamas (via a prohibition notice) where there is a failure to provide protection either by contract or by other methods provided under DPA. The potential damage and distress to any person as a result of an international data transfer, as well as the desirability of facilitating the transfer, will be taken into consideration by the DPC in reaching its decision on whether to permit the transfer. A prohibition notice in accordance with Section 17 of DPA may require the person to take specified steps to protect the interests of the data subject.

A data subject may waive any restriction on international data transfer through their express or implied consent.

4.2 Mechanisms That Apply to International Data Transfers

There are no specific mechanisms that apply to international data transfers from The Bahamas. Under GDC, which is non-binding, it is stated that, subject to the prevailing laws of the Commonwealth of The Bahamas, there are special conditions that must be met before transferring personal data outside the European Economic Arena (EEA) when the importing country does not have data protection laws that are equivalent to that of the EU (as DPA is generally based on privacy principles established by the OECD, UN, EU and Council of Europe). The conditions to consider include the following:

- whether consent was given by the data subject;
- whether the transfer is required under any enactment or by any convention or other instrument imposing an international obligation on The Bahamas (Section 17(8) DPA), pursuant to the performance of a contract between the data controller and a third party and/or data subject; and
- whether the transfer is being made with a view to obtaining legal advice.

4.3 Government Notifications and Approvals

There are no government notifications or approvals required to transfer personal data internationally unless a prohibition notice has been issued with respect to the data by the DPC in accordance with its powers under DPA.

4.4 Data Localisation Requirements

There are no data localisation requirements under DPA.

See **2.2 Sectoral and Special Issues** for data retention requirements relating to financial data.

4.5 Sharing Technical Details

Under the provisions of the Industrial Property Act 1970, an application to the Industrial Property Office (now the Intellectual Properties Section of the Registrar's Office) to register a patent must be accompanied by a specification of the invention, describing it and the methods by which it is to be informed. It is not specifically referenced, though implied, that software code and algorithms would need to be shared in the description of the invention. If the application is granted, the patent will be recorded in the Register of Patents.

4.6 Limitations and Considerations

There is no specific provision under DPA aimed at limiting or prohibiting organisations from collecting or transferring personal data in connection with foreign government data requests, though there are restrictions relating to disclosure pursuant to a foreign government data request. Depending on the jurisdiction and the nature of the investigation, consideration should be given to the Mutual Legal Assistance (Criminal Matters) Act 1990, which provides for the implementation of treaties for mutual legal assistance in criminal matters. The Bahamas currently has a mutual legal assistance treaty with the USA, the United Kingdom and Canada. The Act lays down the process through which foreign courts should make a request (applicable) to the (Bahamian) Competent Authority with a view to obtaining evidence in the jurisdiction to be used in foreign proceedings.

4.7 "Blocking" Statutes

Blocking statutes are not a feature of the Bahamian legislative framework, although the Central Bank of The Bahamas does have the power to block transactions with certain countries in order to meet the international obligations of The Bahamas under various UN and other multilateral sanctions.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

The following emerging technologies (and aspects thereof) are not currently specifically addressed under Bahamian law:

- big data analytics;
- automated decision-making (outside of what has already been discussed in this article);
- profiling (outside of what has already been discussed in this article);
- AI;
- geolocation (outside of what has already been discussed in this article);
- fiduciary duties as they relate to data protection (outside of what would ordinarily be required as a data controller under DPA – where applicable – or under Section 77 of the Banks and Trust Companies Regulation Act 2020 and Section 83 of the Trustee Act 1998); and
- the Internet of Things (IoT).

Biometric Data and Facial Recognition

Biometric data, from a legal standpoint, has only been defined and referred to in legislation within the context of immigration law and biometric cards issued under the Immigration (Amendment) Act 2019, Section 2 of which refers to "biometric data and features" as including digitised fingerprints, machine-readable facial images, machine-readable biographical data and digital signatures.

Drones

Drones (or "unmanned aircraft" or "remotely piloted aircraft") require a permit from the Bahamas Civil Aviation Authority (BCAA), which is a department of the Bahamian Government that has safety oversight of matters pertaining to aviation in The Bahamas. Once an application has been granted, drones are subject to strict altitude restrictions and safety regulations as provided for under Schedule 27 Unmanned and Remotely Piloted Aircraft, the Civil Aviation Act 2016, and Civil Aviation (General) Regulations, 2017.

Disinformation or Other Online Harms

See **2.2 Sectoral and Special Issues**.

5.2 "Digital Governance" or Fair Data Practice Review Boards

There are no known organisations in The Bahamas that establish protocols for digital governance, nor fair data practice review boards or committees that address the risks of merging or disruptive digital technologies outside of URCA, which acts as the electronic communications and telecommunications sector regulator. URCA publishes an Electronic Communications Sector Policy every three years and part of its policy imperatives is to "embrace" emerging technologies. Draft legislation was produced in 2020 with a view to establishing a body corporate called the Virtual Innovation Authority, which would be tasked with, inter alia:

- safeguarding data protection rights;
- developing policies to encourage fair competition;
- assisting vulnerable people through policy;
- promoting fair competition; and
- developing policies in connection with technology risk frameworks and emergent technologies.

This draft legislation, along with the Emergent Technologies Bill, has not progressed any further to date.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation

See **1.2 Regulators** and **1.3 Administration and Enforcement Process**.

There has been no significant private litigation involving privacy or data protection in the last year. It is important to note that class action suits are permissible under Bahamian law but are still largely alien to the litigation culture of The Bahamas, except in the areas of employment law and environmental protection law.

5.4 Due Diligence

When conducting due diligence in corporate transactions, it is imperative to consider any anti-money laundering, counter financing of terrorism and proliferation financing and Know Your Customer regulations and guidelines that may apply or are required to be observed, as provided under the relevant legislation. Consideration should also be taken of any data subject rights afforded to individuals (if applicable) under DPA and any conflict of laws as it pertains to, inter alia, the acceptance of digital signatures for corporate transactions.

5.5 Public Disclosure

As far as is known, there are no non-privacy or data protection-specific laws or regulations that mandate the public disclosure of an organisation's cybersecurity risk profile or experience.

5.6 Other Significant Issues

There are no further significant issues.

Graham Thompson has been one of the pre-eminent law firms in The Bahamas since 1950. The firm operates three offices in The Bahamas (Nassau, Lyford Cay and Freeport) and one in the Turks and Caicos Islands (Providenciales). The firm is internationally recognised for its expertise in the offshore financial arena, including private client, trusts and estates; corporate, commercial and securities; and real estate and development. Graham Thompson's litigators are highly sought-after experts who provide effective, specialised, timely and tailored representation and advice across a wide spectrum of disciplines, including the banking and finance, corporate and commercial, employment and labour, admiralty and shipping, insurance, intellectual property, insolvency, real property and development, regulatory, and manufacturing sectors. Data protection and privacy is also a key practice area for the firm. The attorneys regularly provide regulatory compliance advice to clients, primarily in the financial services, technology, e-commerce, digital media and hospitality sectors.

Author

Sean McWeeney Jr is an associate in Graham Thompson's Financial Services and Private Client Group. He was called to the Bar of England and Wales and the Commonwealth of The Bahamas in 2018. Since joining the firm, his practice has focused primarily on internet law, data privacy compliance, technology, digital media, and e-commerce. Sean is a member of the International Association of Privacy Professionals, the International Technology Law Association, the Bahamas Bar Association, the Internet Society, the Honourable Society of Lincoln's Inn and the Commonwealth Lawyers Association. He recently co-authored an article on the recently enacted Digital Assets and Registered Exchanges Act.

Graham Thompson

Sassoon House
Shirley Street & Victoria Avenue
P.O. Box N-272
Nassau
The Bahamas

Tel: +1 242 322 4130
Email: sgm@gtclaw.com
Web: www.grahamthompson.com

Trends and Developments

Contributed by:
Sean McWeeney Jr and Christina Justin
Graham Thompson see p.20

2020 proved to be a fascinating, if strange, year for data protection and privacy in The Bahamas. With most countries suffering severe economic hardship and uncertainty as a consequence of the COVID-19 pandemic, data privacy became a hot-button issue for governments around the world. In particular, with public health, national security and economic stability being the top priorities for the Bahamian government, civil liberties and privacy rights were inevitably curtailed (via Emergency Powers legislation) as part of the overall effort to contain the spread of the virus. Not surprisingly, this resulted in a great deal of thought and discussion about concepts of privacy and questions as to just how far the curtailment should go in order to mitigate the risks associated with COVID-19.

Quite apart from the COVID-19 phenomenon, however, there were other important legal trends in relation to data privacy, particularly in the fintech space, where The Bahamas has been steadily positioning itself as a global innovator.

COVID-19 Privacy Issues

The COVID-19 pandemic played a central role in most of the major privacy issues that emerged in 2020. Soon after a State of Emergency was declared in The Bahamas and corresponding legislation was enacted (under the successive Emergency Powers (Covid-19 Pandemic) Order(s) and Regulations), health, location and personal data privacy immediately became controversial subjects for national discussion.

At the outset, it is important to note that Section 5 of the Data Protection (Privacy of Personal Information) Act 2003 (DPA) provides that the ordinary protections of the DPA will not apply where personal data – in the opinion of the Minister (with oversight of DPA) or the Minister for National Security – is or was kept for the purpose of safeguarding the security of The Bahamas, or where personal data consists of information that the person keeping the data is required by law to make available to the public. It could be said that in the interest of public health and national security, many of those rights did indeed fall away.

Many of the health and location privacy concerns stemmed from domestic and international travel and the contact tracing that took place once residents returned to The Bahamas and either had exposure to someone that tested positive for COVID-19 or displayed symptoms of COVID-19, or returned from a country that had a comparatively high number of COVID-19 cases. Some privacy concerns surrounding contact tracing revolved around potentially excessive collection, use and retention of data, as well as ensuring that the identity of persons exposed or infected would remain confidential while being transferred to and from various institutions. Collecting such information could lead to the disclosure of highly personal information (going outside the health sphere).

The identities of the first few recorded COVID-19 patients were unfortunately the subject of much social media speculation (including the revelation of not only their identity but also their home addresses, family members and travel history). This eventually led to the creation of a specific provision in the Emergency Regulations criminalising the publication and dissemination of fake news calculated to incite panic, hatred or fear in the community. As a result, the print and electronic media (as well as ordinary purveyors of news on internet platforms such as Facebook) soon adopted the protocol that limited disseminated information to the age, sex, past travel and general status of anonymised patients (ie, dead, hospitalised or under quarantine at home).

The Regulations vested in officers (ordinarily persons designated by the Ministry of Health) the authority to detain and screen persons (if in their judgement that was necessary) for COVID-19, with penalties for failure to comply with health screening protocols. Screenings could also result in the involuntary imposition of a COVID-19 test (or the provision of biological samples) on a suspected COVID victim.

In addition to contact tracing measures, persons returning to The Bahamas would also be subject to electronic monitoring through a mobile phone app (Hubbcat) to facilitate the monitoring of their adherence to quarantine restrictions. In some instances, persons were monitored by the Royal Bahamas Police Force via the Hubbcat app (see below).

Business owners were also required to take the temperature of patrons as a condition for entry to stores and places of business. There have been reported cases of temperature checks (health data) being conducted without patrons' consent, or without any explanation as to what would be done with the temperature data. Many businesses and government offices implemented face-sensing thermometers to conduct temperature checks in place of temperature guns, which also raised privacy concerns as biometric data is not treated as sensitive personal data under DPA as it is in some other jurisdictions.

It has recently been reported that the government is considering issuing a "vaccine passport" for those persons that receive the COVID-19 vaccine once it is made available for Bahamian citizens and residents. It will be interesting to see whether biometric technology will be a component of this rollout and what, if any, privacy issues arise as a result.

Launch of CBDC and Digital Assets Regulation

2020 was an exciting year for fintech in The Bahamas. Project Sand Dollar was inaugurated on 20 October 2020, as part of the Bahamian Payment Systems Modernisation Initiative and with a view to furthering the key objectives of financial inclusion, transaction efficiency, access and diversification of local payment systems (particularly for residents of far-flung Bahamian islands that may not have access to banking facilities). The project was developed by the Central Bank of The Bahamas (CBB) to offer a Central Bank Digital Currency (CBDC) (essentially a digital version of the Bahamian dollar), and followed successful trials in the islands of Abaco and Exuma. Sand Dollar was the first CBDC launched anywhere in the world, and many other jurisdictions are now eager to replicate it.

It should be noted that Sand Dollar is not a cryptocurrency as it is backed by CBB foreign reserves. According to its website, Sand Dollar wallets utilise multi-factor authentication, high-level encryption protocols and enhanced KYC/AML safeguards to maintain the privacy and confidentiality of users and their data. It is also stated that all financial institutions that wish to accept Sand Dollars (including CBB) must undergo an independent cybersecurity assessment to ensure that any technology used in the acceptance of such is up to international standards.

December 2020 also saw the commencement of the long-awaited Digital Assets and Registered Exchanges Act (DARE), which regulates the issuance, sale and trade of digital assets in, or from within, The Bahamas. DARE further provides legal recognition for emerging technologies and fintech instruments, such as distributed ledger technology (eg, blockchain), the digital token exchange, initial token offering and virtual currency tokens. Consequently, The Bahamas has now joined only a handful of jurisdictions that have sought to regulate this emerging industry. Notably, Section 4 of DARE stipulates that the Act must be administered by the Securities Commission of The Bahamas (SCB). SCB thus serves as regulator, monitor and supervisor of the issuance of digital assets, digital asset businesses and related activities that fall under the ambit of DARE.

The issue of data protection is addressed in Part III of DARE, with particular focus on data retention and the prevention of unauthorised access. Registrants under DARE are statutorily obligated by Section 23 to take and maintain record-keeping measures that ensure the accurate collection of information and documents. Registrants must also implement data protection measures that are in line with DPA to protect the personal data of their customers.

Lastly, data protection measures must be specified within a Registrant's offering memorandum (OM) in connection with an initial token offering. This forms an integral part of an issuer's duty to provide full and accurate pertinent information that would allow potential purchasers to make informed decisions. The OM is to be posted on the issuer's website for the perusal of potential purchasers for the duration of the offering period.

Examples of data protection and privacy measures that should be addressed in the OM include, but are not limited to, the following (in accordance with Item 7, Second Schedule of DARE):

- a description of security safeguards with a view to preventing cyber-threats to the underlying protocol, off-chain activities and any wallets issued by the issuer;
- standards of any smart contracts used or deployed by the issuer;
- a description of any program agents used to obtain data and verify occurrences from smart contracts; and
- a description of any intellectual property rights associated with the offering, and protection thereof.

Biometrics and Surveillance

Biometrics

It has already been noted that the use of biometrics and surveillance increased in 2020 as a result of the pandemic. There is still a notable lack of legislation regulating the collection, use and retention of biometric data, despite the growing popularity of mobile apps, software and services utilising biometric identifiers to authenticate a user's identity. Again, biometrics are not classified as sensitive personal data under DPA as they are in some other jurisdictions, so such data would be treated in the same manner as standard personal data. We would submit that this lacuna is in need of legislative remediation.

The definition of "biometrics data and features" in the Immigration (Amendment) Act 2019 would include digitised fingerprints, machine-readable facial images (eg, facial recognition), machine-readable biographical data and digital signatures. To this end, and in light of the government's efforts to deepen and extend the digital transformation of e-government services, foreign nationals residing and/or working in The Bahamas now receive biometric immigration cards (this follows the issuance of biometric Bahamian passports, national health insurance cards and driver's licences). Enactments of the Bail (Amendment) Act 2020 and Parliamentary Elections (Amendment) Act 2020 also pave the way for bail applications to be made using one's biometric data via an electronic bail management system,

and for the issuance of biometric voter cards to use in future elections or referenda.

Sand Dollar also utilises biometric recognition technology such as facial recognition as part of its identity verification and authentication process. Some concerns have been raised that existing data protection laws are not robust enough to adequately address the data privacy issues that could arise from the collection and retention of personal data such as purchase/transaction history, biometrics and geolocation by a State-owned entity (CBB), or where there are multiple data controllers involved in the overall transaction. For example, The Bahamas does not impose a positive duty on data controllers to notify data subjects in the event of a data breach. For this reason, it is expected that any amendments to existing cyberlaws (or new legislation specifically aimed at regulating Sand Dollar) will include updated classifications of personal data to provide more protection for data subjects.

Surveillance

Surveillance became a controversial issue during the initial onset of COVID-19 when the Royal Bahamas Police Force (RBPF) opened the Hubbcat Centre to participate in the electronic monitoring of persons required to quarantine, while the Ministry of Health monitored individuals who had actually tested positive for COVID-19. At that time, concerns were expressed about whether police surveillance went too far in the overall monitoring of the movement of quarantined individuals and the attendant curtailment of private home life and freedom of movement.

Surveillance relating to crime and national security, however, also became the subject of several news items in 2020/1. Recently, a Real-Time Crime Centre was established by the RBPF and will serve as its police tech hub. This will include the monitoring of, inter alia:

- the RBPF's expanded CCTV coverage (the assumption being that facial recognition technology will be used to facilitate identifying suspected perpetrators of crimes);
- aerial technology (the RBPF has contracted with a company to use unmanned, remote-controlled surveillance and disaster relief drones in the near future); and
- ShotSpotter (technology used to detect when and where a firearm has been discharged).

Lastly, pursuant to the commencement of the National Crime Intelligence Agency Act 2019 (NCIA Act) in January 2020, it was recently announced that a National Crime Intelligence Agency (NCIA) will become operational in 2021. Section 5 of the NCIA Act states that the main functions of NCIA will include collecting intelligence by investigation or otherwise where strictly necessary, and analysing and retaining intelligence related to activities that may constitute threats to the security of The Bahamas. The NCIA Act also applies extra-territorially in that performance of NCIA functions may take place within or outside the jurisdiction. It will be interesting to see what kinds of privacy issues might arise as a result of NCIA becoming fully operational and what impact it will have on the crime rate.

Revenge Porn

Revenge porn can be described as a form of digital or electronic abuse that is perpetrated through the distribution of sexually explicit material without the consent of a subject of the video or images. In many instances, the material is intentionally leaked to social media platforms or through online messaging platforms in an effort to cause or bring humiliation, ridicule or shame to the victim (typically a former love interest, sexual partner or desired sexual partner). Under Bahamian law, crimes of this nature are typically charged as "intentional libel" under the provisions of the Penal Code as there is no legislation that specifically addresses the issue of revenge porn.

Fortunately, 2020 saw a continued trend of the courts taking revenge porn very seriously. In February 2021, it was reported that a man was sentenced to nine months in prison after being accused of distributing sexually explicit images of a former partner to her co-workers out of revenge for not allowing him to see their child. The images were reportedly screenshots taken during a nude video call and the complainant had not consented to them being released.

A similar sentence was handed down in April 2020 in the case of a man who had posted a sexually explicit video of a former partner to her co-workers and former schoolmates, which was later spread across social media. Despite the act having reportedly been recorded consensually, it was also reported that the man's former partner had not consented to the video being shared. The man received a six-month sentence for his actions from the Magistrates Court.

These cases illustrate that the courts take revenge porn matters seriously and will not hesitate to send digital abusers to jail for their actions. It will be interesting to see if revenge porn is specifically addressed in future legislation or treated as an extension of domestic abuse, given its psychological and abusive characteristics.

Notable Data Breaches

The Financial Crimes Investigation Unit of The Bahamas reported a notable increase in cybercrimes in 2020, particularly after the onset of COVID-19 in March of that year. Hacking, fraud and extortion incidents were specifically mentioned as showing marked increases.

For many corporations and businesses (small, medium and large), the pandemic has certainly stressed the importance of having adequate cybersecurity safeguards in place to protect client, patient and/or customer personal data in the event of a cyber-incident. As much of the workforce and student population shifted to remote online platforms, this left some businesses and institutions vulnerable to hackers looking to exploit (and capitalise on) weak cybersecurity infrastructures.

One particularly heinous data breach occurred in early April 2020 after a confidential document containing a list of names of persons purportedly receiving HIV/AIDS treatment at Grand Bahama Health Services (Rand Memorial Hospital) was leaked onto social media and circulated on various communications platforms. It was not immediately clear who was responsible for this data leak, what their motives were for disseminating the list, or how they were able to obtain it. In any event, the Public Hospitals Authority (PHA) swiftly engaged the RBPF and launched a criminal investigation into the matter, later issuing a press statement reminding the public that patient health records are confidential and cannot be shared without the patient's consent. PHA also rightly emphasised that leaking such data contravenes various provisions of DPA.

Another widely reported cybersecurity incident concerned a hacking and subsequent publishing of company filings information housed on a server used by the Registrar General's Department. While the business registration platform was compromised, it is important to note that the information leaked from the server is ordinarily accessible to the public for a fee. The hacking was perpetrated by Distributed Denial of Secrets, a non-profit whistle-blower site and so-called "transparency collective" that has been compared to Wikileaks. The hack took place in early January 2020, but the public did not become aware of the incident until June of the same year.

As the hacking of computer systems and unauthorised access to data stored thereon are criminal offences under the Computer Misuse Act, DPA and Penal Code respectively, a police investigation was launched to investigate the matter, in conjunction with a review of the existing digital security infrastructure. It has since been reported that part of the government's digital transformation initiative includes upgrading existing servers to enhance their security.

Remote Work and Employee Monitoring

In The Bahamas, as with many other places around the world, non-essential businesses were mandated to work remotely. As a result, there was a major shift toward digital presence and electronic services on many available platforms. Business owners sought advice on cybersecurity and data protection issues, legally or otherwise, as many became more concerned with securing and protecting the information of their employees and clients.

Despite concerns, after a year of the "new normal", many Bahamians grew accustomed to remote working, with at least 60% of Bahamians now preferring to work from home, according to various surveys.

National Cybersecurity Strategy and Expected Changes to Cyberlaws

In response to increased electronic communications and recent cyber-attacks, The Bahamas government partnered with the International Telecommunications Union (ITU) to launch the National Cybersecurity Project. The team intends to implement a national cybersecurity strategy and establish a Computer Security Incident Response Team.

While not many details surrounding the project have been made available to the public at this stage, the team acknowledges that data protection and cybersecurity legislation is in need of urgent review. The most recent data study from UN Global Cybersecurity Index revealed that The Bahamas is ranked 133rd out of 193 countries for cybersecurity. As the Bahamian government continues various modernisation and digitisation initiatives, we are looking forward to significant legislative reform in the data privacy sector in the coming years.

URCA Electronic Communications Policy 2020–2023

The Utilities Regulation & Competition Authority (URCA – the regulatory body for electronic communications in The Bahamas) has released its new Electronic Communications Sector Policy for 2020–2023. The policy is mainly aimed at informing the public of government objectives for the electronic communications sector, and providing a regulatory framework that supports these objectives.

One major takeaway from the policy is the government's delivery of digitised government services to the public. More often than not, Bahamians experience government services through multiple isolated channels due to a lack of inter-departmental cohesiveness and communication. Though this problem has pervaded Bahamian society for decades, it was exacerbated by the COVID-19 pandemic. By launching this project, the government intends to establish a fully digitised and integrated process for the provision of public government services. The digitisation overhaul is referred to as electronic government, or "e-government".

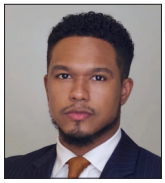
Also of major significance for those in the data privacy realm is the government's intention to digitise the healthcare system through computerising records and inventory to ensure, among other things, "easy retrieval of patient records".

Electronic Signatures Now Extending to Deeds

Pursuant to the Property (Execution of Deeds and Documents) Act of 2020, a deed may now be validly executed by way of electronic signature. In this regard, the Companies Act was also amended to allow for deeds to be executed electronically by an authorised individual on behalf of the company. This supplements and extends earlier legislation that allowed for the electronic signature of most non-deed documents.

Graham Thompson has been one of the pre-eminent law firms in The Bahamas since 1950. The firm operates three offices in The Bahamas (Nassau, Lyford Cay and Freeport) and one in the Turks and Caicos Islands (Providenciales). The firm is internationally recognised for its expertise in the offshore financial arena, including private client, trusts and estates; corporate, commercial and securities; and real estate and development. Graham Thompson's litigators are highly sought-after experts who provide effective, specialised, timely and tailored representation and advice across a wide spectrum of disciplines, including the banking and finance, corporate and commercial, employment and labour, admiralty and shipping, insurance, intellectual property, insolvency, real property and development, regulatory, and manufacturing sectors. Data protection and privacy is also a key practice area for the firm. The attorneys regularly provide regulatory compliance advice to clients, primarily in the financial services, technology, e-commerce, digital media and hospitality sectors.

Authors



Sean McWeeney Jr is an associate in Graham Thompson's Financial Services and Private Client Group. He was called to the Bar of England and Wales and the Commonwealth of The Bahamas in 2018. Since joining the firm, his practice has focused primarily on internet law, data protection and privacy compliance, technology, digital media, and e-commerce. Sean is a member of the International Association of Privacy Professionals, the International Technology Law Association, the Bahamas Bar Association, the Internet Society, the Honourable Society of Lincoln's Inn and the Commonwealth Lawyers Association. He recently co-authored an article on the recently enacted Digital Assets and Registered Exchanges Act.

Christina Justin is an associate in Graham Thompson's Litigation and Dispute Resolution Group. She was admitted to the Bar of England and Wales and the Bahamas Bar in 2015, and to the New York Bar in 2020. She is an active member of the American Bar Association and the Bahamas Bar Association. Her practice is focused mainly on commercial litigation and providing advice to financial institutions on commercial and transactional issues. She is also expanding her litigation and dispute practice to include matters concerning data privacy and electronic communications in The Bahamas.

Graham Thompson

Sassoon House
Shirley Street & Victoria Avenue
P.O. Box N-272
Nassau
The Bahamas

Tel: +1 242 322 4130
Email: sgm@gtclaw.com
Web: www.grahamthompson.com