OFFICE OF THE

DATA

PROTECTION COMMISSIONER

Annual Report

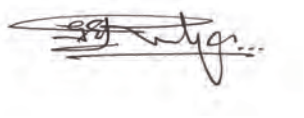
2012

The Honourable Perry G. Christie
Prime Minister & Minister of Finance
Cecil V. Wallace-Whitfield Centre
Cable Beach
P.O. Box N-3017
Nassau, N.P.
The Bahamas

Dear Prime Minister,

In compliance with Section 21 of the Data Protection (Privacy of Personal Information) Act, 2003, I am pleased to submit to you, for presentation to Parliament, the sixth Annual Report on the activities of the Office of the Data Protection Commissioner for the reporting year ended December 31st 2012.

Yours faithfully,



George E. Rodgers
Data Protection Commissioner

February, 2013

WHAT IS DATA PROTECTION?

Data Protection is the safeguarding of the privacy rights of individuals in relation to the processing of personal information. The Data Protection (Privacy of Personal Information) Act, 2003 ("The Data Protection Act") places responsibilities on those persons processing personal information, and confers rights upon the individuals who are the subject of that information. The Data Protection Act also sets out the legal framework for the collection, use and disclosure of personal information that is consistent with international principles recognized by the Council of Europe, [The European Union (EU)] and the Organization for Economic Cooperation and Development (OECD), and the United Nations (UN).

From our point of view, the key principle of data protection is that living individuals should be able to control how personal information about them is used, with or without their consent.

"It is far easier to defend privacy while you still have it, than to reclaim it once it has been lost." (Emma Martins, Data Protection Commissioner, Jersey, Channel Islands).

LIST OF ABBREVIATIONS

CARTAC	- Caribbean Regional Technical Assistance Centre
CBB	- Central Bank of The Bahamas
CCTV	- Closed Circuit Television
CMA	- Computer Misuse Act, 2003
DPA	- Data Protection (Privacy of Personal Information) Act, 2003
ECTA	- Electronic Communications and Transactions Act, 2003
EU	- European Union
FOI	- Freedom of Information Act, 2012
HTTP	- Hypertext Transfer Protocol
IFC	- International Finance Corporation
IRC	- Internet Relay Chat
OAG	- Office of the Attorney General
ODPC	- Office of the Data Protection Commissioner
OECD	- Organization for Economic Cooperation and Development
PSAs	- Public Service Announcements
UK	- United Kingdom
UN	- United Nations

CONTENTS

FOREWORD

This is my sixth report as Data Protection Commissioner for the Commonwealth of The Bahamas. It covers the year 2012. The Data Protection (Privacy of Personal Information) Act, 2003, (DPA) has been in force since 2nd April, 2007 and with the passing of 2nd April, 2012, the final grace period for all participants to be in full complaince has expired. This final period was defined by Section 31 (2) which mandated in part that:-

"Government agencies and other bodies specified in the First Schedule may continue for a period of five years from the date of entry into force of this Act, to use and process existing files that contain personal data including sensitive personal data which were acquired in circumstances in which it is not possible to determine if such was obtained in pursuance of a legal obligation or with the consent of the data subjects."

I therefore urge all stakeholders to revisit the personal data files in their care to ensure that there are no surprises present beforehand in the event a formal access request is made under Section 8 of the DPA. You should bear in mind that once an access request is made it is a criminal offence to alter; remove; destroy, or otherwise deny access to material on file.

Data Protection (Privacy) in 2012 continued to be a moving target because of fast moving technological and social change. Organizations around the world continue to be hit with headlines about phone-hacking and inappropriate disclosure of personal information; The Bahamas is no exception. The passage of time has proven that we must do more to balance the rights of privacy and freedom of expression. While legislation passed in 2003 along with the DPA [(The Computer Misuse Act (CMA) and the Electronic Communications and Transactions Act (ECTA)] do much to support the work of the Office of the Data Protection Commissioner (ODPC); the Freedom of Information Act, 2012 (FOI) once enacted, will provide the impetus for balance when dealing with privacy issues.

Arguably, while clearly providing the majority of users with a positive experience, there is a darker side to the use of social media when it is used for "unfriendly purposes." From cyber-bullying to stalking, we are seeing the pre-internet statutory frameworks struggling to respond to the dramatically changing technological landscape. But respond we must and privacy authorities around the world, notably the European regulatory partners are giving these concerns due consideration.

Bahamians continue to put more of their personal information on-line and so the need for more education in this regard is apparent. The ODPC continues to use our "Tip of the Month" feature to highlight some of these concerns. More will be said about this subject later in this report.

It is important to remind all that the DPA mandates that the Commissioner is independent in the performance of his duties and has privacy responsibility for:-

- administering and enforcing the provisions of the DPA;
- promoting the observance of good practice methods by Data Controllers within the requirements of the DPA;
- influencing thinking on privacy and processing of personal information matters on a local and global basis; and
- discharging as the national supervisory authority, various functions relating to or arising from any international obligations The Bahamas may have or is seeking to be a party to, in connection with data protection.

Our aim is to be responsive and proactive to data protection (privacy) issues as much as we can within our resource capability. This is where the real challenge remains; the continuous use of best practices in the field of data protection and keeping abreast of developments in privacy and related industries are some of the key measures we can tap into in fulfilling our mandate.

COMMISSIONER'S STATEMENT

2012 represents the sixth and perhaps my final year as Data Protection Commissioner for the Commonwealth of The Bahamas. I am pleased to present Annual Report 2012.

Our mandate to promote and protect the privacy rights of individuals will soon become more challenging with the passage of the Freedom of Information Act, 2012 (FOI). By virtue of Part VI Section 35 of FOI the responsibilities of the new "Information Commissioner" will be combined with those of the Data Protection Commissioner who will now be one and the same person. Although not yet activated, FOI will usher in a huge culture change requiring a change in attitude to provide information rather than seeking ways of withholding it. ***Appendix 1*** provides commentary on the new FOI legislation in the form of an opinion by Mrs. Rowena G. Bethel, which has already been widely circulated.

For a successful implementation of FOI there must also be an ability and willingness to comply with the requirements of the FOI by all agencies involved in the process. With the introduction of a freedom of information regime, there will be a greater need for "balance" between the citizen's right to public information and the individual's right to privacy. The message remains one of caution. Personal information is extremely valuable and should be treated as such. It is more important than ever for citizens to make sure they deal with reputable organizations, use privacy settings and only make financial transactions on secure sites. Individuals must also do more to protect themselves. The data protection law is on your side, the Data Protection Commissioner can only help you if you reach out to him in the form of making formal complaints for investigation.

A new format of Website Statistics was available for some six months of the year (covering the first two months – January and February, 2012 then again from October, 2012 to January, 2013). This information indicated a count in excess of 13,400 hits which was a substantial improvement over a similar period last year (2,687). Going forward we expect that statistics will be captured on a consistent basis providing a more accurate measure of the effectiveness of our Website. Refer to **Appendix 2** for a graphic display of the available information.

I am pleased to report marginal gains in other statistics with six (6) complaints and thirty-seven (37) queries being received. This compares with five (5) complaints and thirty (30) queries in 2011. On the other side of the coin there were only eight (8) road trips and three hundred and eight (308) individual interactions during the year (prior year-sixteen (16) road trips and three hundred and ninety-four (394) individuals). Road trips were severely affected as several Family Island destinations were cancelled due to the passage of Hurricane Sandy. **(See Appendix 3 - Schedule of Visits and/or Presentations).**

The 34th International Conference of Data Protection and Privacy Commissioners was held in Punta Del Este, Uruguay, during the week of 23rd October, 2012. While I did not attend the event this year, I was able to secure copies of the resolutions that were passed at the close of the event. There were three (3) main topics covered by the resolutions:

1. **Resolution** – on profiling; looking at the ever growing amount of data being collected and processed by both private and public authorities around the world (the so – called big data).

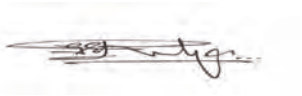
2. **Resolution** – on the future of privacy and what is being done to protect it.

3. **Resolution** – on Cloud Computing and its increasing ability to attract interest therein due to the promise of greater economic efficiency, lower environmental impact, simpler operation, user friendliness and a number of other benefits.

See the full text of these resolutions at www.privacyconference2012.org

As the data protection authority for The Bahamas, the ODPC is obliged to note that the ground work to be able to submit an application to the European Commission, an agency of the European Union (EU) for an assessment of our regime with a view to satisfying the EU adequacy test for transborder flows remains before us. The enactment of the DPA overcame the first hurdle. Secondly, our efforts to produce a set of Regulations arising from the DPA continue. Thirdly, we continue to encourage our community to take advantage of our facilities to enhance our Case Management Skills. In addition to the above, our Law Reform and Revision Commission have been asked to produce a set of Regulations to accompany FOI.

Finally, I take this opportunity to thank the Acting Financial Secretary Mr. Ehurd Cunningham for his continued support to the work of the ODPC. I would also like to thank Mrs. Rowena G. Bethel for her contribution at ***Appendix 1.*** Very special thanks to my Secretary, Mrs. Sabrina Martin and Mr. Dexter Fernander, for their untiring assistance and technical support in producing this Report.



George E. Rodgers
Data Protection Commissioner

February, 2013

SELECTED TERMINOLOGY IN THE DATA PROTECTION (PRIVACY OF PERSONAL INFORMATION) ACT, 2003

The following terminology is used where it relates to our data protection legislation:-

"Data" means information in a form in which it can be processed.

"Data Controllers" means a person who (either alone or with others) determines the purposes for which and the manner in which any personal data are, or are to be processed.

"Data Processor" means a person who processes personal data on behalf of a Data Controller but does not include an employee of a Data Controller who processes such data in the course of his employment.

"Personal Data" means data relating to a living individual who can be identified:-

(i) from the data, or

(ii) from the data and other information or data in possession of the data controller.

"Processing" in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data including:-

(i) organization, adaptation or alteration of the information or data;

(ii) retrieval, consultation or use of the information or data;

(iii) transmission of data;

(iv) dissemination or otherwise making available, or

(v) alignment, combination, blocking, erasure or destruction of the information or data.

"Data Subject" means an individual who is the subject of personal data.

"Back-up Data" means data kept only for the purpose of replacing other data in the event of their being altered, lost, destroyed or damaged.

DATA PROTECTION

A Quick Guide

What is the Data Protection Act?

The Data Protection (Privacy of Personal Information) Act, 2003 (DPA) seeks to strike a balance between the rights of individuals and the sometimes "competing" interests of those with legitimate reasons for using personal information. The DPA gives individuals certain rights regarding information held about them. It places obligations on Data Controllers (those who process information) while giving rights to Data Subjects (those who are the subject of that data). Personal information covers both facts and opinions about the individual.

1. **Rights of Individuals under the DPA.**

   Individuals have a number of legal rights under The Bahamas' data protection law. You can…

   - expect fair treatment from organizations in the way they obtain, keep, use and share your information;
   - subject to prescribed exceptions, demand to see a copy of all information about you kept by the organization;
   - stop an organization from using your details for direct marketing;
   - demand that inaccurate information about you be corrected;
   - demand that any information about you be deleted, if the organization has no valid reason to hold it;
   - complain to the Data Protection Commissioner if you feel your data protection rights are being infringed;
   - sue an organization through the courts if you have suffered damage through the mishandling of information about you.

2. **Obligations on Data Controllers under the DPA**.

   To comply with their data protection obligations Data Controllers must:

   - collect and process information fairly;
   - keep it only for one or more specified, explicit and lawful purposes;
   - use and disclose it only in ways compatible with these purposes;
   - keep it safe and secure;
   - keep it accurate, complete and up-to-date (except for back-up data);
   - ensure that it is adequate, relevant, and not excessive;
   - retain it no longer than is necessary, except for historical, statistical or research purposes;
   - subject it to prescribed exceptions, give a copy of his/her personal data to any individual, on request

DATA PROTECTION PRINCIPLES AND HINTS OF THEIR USAGE

The DPA incorporates several principles that safeguard the collection, use and disclosure of personal information. Data Controllers have legal responsibilities arising from these principles and a "Yes" answer to the following questions should help readers to develop a clear policy statement on data protection for their organizations.

Principle 1: Collect personal data by means which are lawful and fair.

- At the time when we collect information about individuals, are they made aware of the uses for that information?
- Are people made aware of any disclosures of their data to third parties?
- Have we obtained people's consent for any secondary uses of their personal data, which might not be obvious to them?
- Can we describe our data-collection practices as open, transparent and up-front?

Principle 2: The data must be accurate and up-to-date (except in the case of back-up data).

- Do we check our data for accuracy?
- Do we know how much of our personal data is time-sensitive, i.e. likely to become inaccurate over time unless it is updated?
- Do we take steps to ensure databases are kept up-to-date?

Principle 3: The data shall be kept only for one or more specified and lawful purpose(s).

- Are we clear about the purpose (or purposes) for which we keep personal information?
- Are the individuals on our database also clear about this purpose?

Principle 4: The data shall not be used or disclosed in any manner incompatible with that purpose or purposes.

- Are there defined rules about the use and disclosure of information?
- Are all staff aware of these rules?
- Are the individuals aware of the uses and disclosures of their personal data? Would they be surprised if they learned about them? Consider whether the consent of the individuals should be obtained for these uses and disclosures.

Principle 5: The data shall be kept accurate, relevant and not excessive in relation to that purpose or those purposes.

- Do we collect all the information we need to serve our purpose effectively, and to deal with individuals in a fair and comprehensive manner?
- Have we checked to make sure that all the information we collect is relevant, and not excessive, for our specified purpose?
- If an individual asked us to justify every piece of information we hold about him or her, could we do so?
- Does a policy exist in this regard?

Principle 6: The data shall not be kept for longer than is necessary (except in the case of personal data kept for historical, statistical, or research purposes).

- Is there a clear statement on how long items of information are to be retained?
- Are we clear about any legal requirements on us to retain data for a certain period?
- Do we regularly purge our database of data which we no longer need, such as data relating to former customers or staff members?
- Do we have a policy on deleting personal data as soon as the purpose for which we obtained the data has been completed?

Principle 7: Appropriate security measures shall be taken against authorized access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction.

- Is there a list of security provisions in place for each data set?
- Is someone responsible for the development and review of these provisions?
- Are these provisions appropriate to the sensitivity of the personal data we keep?
- Are our computers and our databases password-protected, and encrypted if appropriate?
- Are our computers, servers, and files security locked away from unauthorized people?

Principle 8: The Right of Access.

- Is a named individual responsible for handling access requests?
- Are there clear procedures in place for dealing with such requests?
- Do these procedures guarantee compliance with the DPA requirements?

The above eight (8) principles should be supported by adequate training and education through a coordinated effort and compliance by all stakeholders:-

Training & Education

- Do we know about the level of awareness of data protection in our organization?

- Is our staff aware of their data protection responsibilities – including the need for confidentiality?
- Is data protection included as part of the training programme for our staff?

Coordination and Compliance

- Has a data protection coordinator and compliance person been appointed?
- Are all staff aware of his or her role?
- Are there mechanisms in place for formal review by the coordinator of data protection activities within our organization?

Having examined yourself on the above, the final question is “Are you ready for data protection?”

THE COMMISSIONER AT WORK

Promoting Public Awareness

You will note from our "Tip of the Month" feature **(Appendix 4)** that the focus has been on protecting the privacy rights of individuals in an environment where the use of social media is fast out-pacing the more traditional means of communication. Consequently, in order to fully participate in this arena we have successfully launched a "Facebook" page under the banner of "Office of the Data Protection Commissioner." A Twitter account is expected to follow in due course.

These media will allow us to quickly comment on current issues and help to develop and promote a culture in which personal information is protected and respected.

The topics covered throughout the year with this in mind are still accessible on our Website at www.bahamas.gov.bs/dataprotection under the heading "Tip of the Month Archives."

The DPA applies to almost every data controller in The Bahamas and because some have sought to escape its purview, it is fitting that we detail below the contents of Section 4 of the DPA which speaks to its application as under:-

1. The act applies where a data controller:-

    (a) is established in The Bahamas and the data are processed relevant to that establishment; or

    (b) the data controller is not established in The Bahamas but uses equipment in The Bahamas for processing the data otherwise than for the purpose of transit through The Bahamas.

2. A data controller who fits the description of (1) (b) must nominate a representative established in The Bahamas to comply with the DPA.

3. For the purposes of (1) and (2) above, each of the following is to be treated as established in The Bahamas:-

    (a) an individual who is ordinarily resident in The Bahamas;
    (b) a body incorporated or registered under the laws of The Bahamas;
    (c) a partnership or other unincorporated association formed under the laws of The Bahamas; and
    (d) any person who does not fall within paragraph (a), (b) or (c) but maintains in The Bahamas an office, branch or agency through which he carries on any business activity or a regular practice.

There are also some specific exclusions under the Act and these have been enumerated in Section 5 of the DPA which states that the Act shall not apply to personal data:-

(a) that in the opinion of the Minister or the Minister for National Security are, or at any time were, kept for the purpose of safeguarding the security of The Bahamas;
(b) consisting of information that the person keeping the data is required by law to make available to the public;
(c) kept by an individual and concerned only with the management of his personal, family or household affairs or kept by an individual only for recreational purposes;
(d) deliberations of Parliament and Parliamentary committees; or
(e) pending civil, criminal or international legal assistance procedures.

We consider it is important to remind the public specifically of the foregoing. It is also imperative that resources be made available to mount a fresh promotion campaign. Such a campaign consisting of Public Service Announcements (PSAs) via radio, television and newsprint will certainly broaden the appeal and appreciation for the principles of data protection and the privacy of individuals. Furthermore, the addition of FOI will demand and stimulate the promotion of an effective awareness campaign covering both data protection and freedom of information.

Six (6) formal complaints were received during the year 2012, accompanied by thirty-seven (37) queries via the telephone and e-mail, compared to five (5) formal complaints and thirty (30) queries in 2011. Of the six formal complaints recorded:-

- two related to prolonged response to access to personal information.
- there were two outright denial of access to personal information.
- the remaining two centered around unauthorized disclosure of personal information.

Five of these were successfully resolved while one remains under investigation by the Commissioner and is the subject of an ongoing matter before the Supreme Court.

Promoting Public Education

During 2012 the Commissioner made eight (8) road trips/presentations to schools and the religious community. Through this medium, client contact was made with three hundred and eight (308) individuals; this compares with sixteen (16) visits and three hundred and ninety-four (394) individuals the year before. (See Appendix 3 for a Schedule of Visits and/or Presentations). As mentioned previously, the reduction in road trips etc. was due to the impact of Hurricane Sandy in the Family Islands which were the planned focus of scheduled visits that had to be aborted.

Perhaps one of the most powerful educational tools for individuals is an appreciation of the value of their personal information. You must think before you give out personal information, asking what it will be used for once received. In this regard we again reference our Tip of the Month feature **(Appendix 4)** where we seek to bring alive various topical advice for our citizenry.

This year we have added a new "Education Cover" **(Appendix 5)** which seeks to give you a handle on developing terms used in the industry to describe various activities.

There is an ongoing vibrant debate about the relevance of privacy (data protection) in a world where technology seems to overpower our ability to remain anonymous. President Barack Obama, USA puts this in perspective when he stated:-

> "One thing should be clear, even though we live in a world in which we share personal information more freely than in the past, we must reject the notion that privacy is an outmoded value."

We offer the below additional tips to help you protect your privacy:-

- Don't be afraid to ask to see any personal information held about you. If it's wrong, ask for it to be corrected.
- Don't allow yourself to be pressured into buying things by mail or over the phone.
- Help keep your kids safe online by encouraging them to talk to you about what they're doing.
- Protect yourself from identity theft by ripping up your personal letters and bills etc. when they are no longer required. Use a shredder, if possible.
- Limit your risk when buying online. Have a separate, low-limit credit card.
- Posting personal information on the internet. Use a nickname if you can.
- Check security procedure in internet cafés and make sure you log out before you leave.
- Make sure you've got up-to-date safety software on your computer, especially if you're doing banking online.

Protecting the Public

The Commissioner is a member of the Special Advisory Committee on Closed Circuit Television (CCTV). Work continues on this national project which has encountered some delay but is still expected to come to fruition by mid-2013. The committee has been provided with a set of data protection (privacy) protocols which have been incorporated into the work plan for the project.

Work continues on the establishment of a Credit Bureau in The Bahamas. Locally, the project is headed by the Central Bank of The Bahamas (CBB). It is part of a project by the Caribbean Regional Technical Assistance Centre (CARTAC) that involves integrating the CBB into the International Finance Corporation's (IFC) regional initiative to provide technical assistance for the establishment of a credit bureau. The Data

Protection Commissioner is monitoring this process and has participated in several of the ongoing discussions to ensure the privacy rights of our citizenry are protected. At this stage the legal framework for this project has been drafted and is presently under review. In addition, a draft Credit Reporting Knowledge Guide with input from various stakeholders has been produced under the auspices of the IFC. The guide aims to support best practices in credit reporting development based on IFC experiences in the Caribbean region.

With the enactment of the Freedom of Information Legislation (FOI) and the Data Protection Legislation (DPA) we await the accompanying set of Regulations, for each piece of legislation which are within the purview of the Law Reform and Revision Commission; a division of the Office of the Attorney General (OAG) of the Commonwealth of The Bahamas.

We reiterate that data protection and freedom of information go hand in hand. Administrated together with purpose and ”balance” strengthened by a strong commitment to independence, the benefits afforded to all stakeholders will be immeasurable.

Finally, be it known that all grace periods allotted under Section 31 of the DPA have expired. The ODPC is available to answer questions about your privacy concerns and help you to protect your personal information.

After all … “Privacy Remains the Best Policy!”

DUTIES OF THE COMMISSIONER

1. To promote the observance of good practice by Data Controllers with the requirements of the DPA.

2. To provide information to the public about the legislation, how it works, and about other matters relevant to the work of the Office.

3. To issue codes of practice for guidance as to good practice about data protection where the Commissioner considers it appropriate subject to appropriate consultation. The Commissioner is also required, in appropriate cases to encourage the preparation and dissemination of data protection codes of practice by trade associations, consider those codes submitted to him, ensure appropriate consultation and then provide an opinion on the code as to good practice.

4. Annually, to prepare and cause a report in relation to his activities under the DPA to be laid before each House of Parliament in accordance with section 21 of the DPA.

5. To investigate any contravention of the DPA. The Commissioner is required to investigate whether any contravention has occurred in relation to an individual, either of his own volition or as a result of a complaint by an individual concerned.

6. To discharge, as the national supervisory authority, various functions relating to, or arising from any international obligations The Bahamas may have or is seeking to be a party to, in connection with data protection.

7. To keep proper accounts and other records in relation to the accounts, to prepare an annual Statement of Account in the form required by the Minister, with the consent of the Minister of Finance and to send copies of that Statement of Account to the Auditor General.

8. To designate from his staff at the relevant time, someone to perform his functions during any temporary absence.

9. To perform all other functions and exercise such powers as are reasonably and legally contemplated by or necessary for giving full effect to the provisions of the DPA and for its due administration.

See **Appendix 5** for details of "Organization by Functions."

POWERS OF THE COMMISSIONER

1. ***Enforcement powers*.*** These include service of information notices (S.18) and enforcement notices (S.16), to enable the Commissioner to investigate and rectify instances of non-compliance with:

    - any of the data protection principles,
    - any other requirements of the DPA.

2. ***Transborder data flows*.*** The Commissioner has power to issue prohibition notices, prohibiting the transfer of personal data in circumstances where the data would lose its protections under the DPA. (S.17).

3. To prosecute any offence under the DPA together with associated powers of entry and inspection in connection with the investigation of any such offence (or contravention of any of the data protection principles).

*** NB. All notices are subject to appeal to the Supreme Court under Section 24.**

COMMENTARY ON THE FREEDOM OF INFORMATION ACT, 2012

By: Rowena G. Bethel

In February, 2012, just prior to General Elections, the Freedom of Information Act 2012 ("the Act") was passed into law.

The Act seeks to introduce a revolutionary approach, in the Bahamian context, to the conduct of government affairs by opening the process to general public scrutiny. In keeping with international standards, this is intended to enable greater engagement by the public in government policy formulation and decision-making; and permit better monitoring of the administration and management of government affairs. Currently over ninety countries across the world have introduced such a framework.

The Act has not yet been brought into force and will require significant change in disclosure policies and processes governing access to non-public information held by government and certain designated non-governmental authorities. The Act received considerable criticism during its passage through Parliament due to the lack of consultation within and outside the government machinery, on its development and content.

The right to access non-public government information

The Act grants Bahamian citizens and residents a general right to access information held by central government and its agencies and other designated entities performing public sector type functions or which are substantially funded by the Government. The Act does provide exceptions to this general right by expressly exempting from disclosure certain defined categories of information. As an observation it would appear that on balance the general right of access under the Act seems to have been significantly circumscribed by various exclusions, exemptions, prerogatives to deny access to information, ministerial vetoes and preservation of the access rules under the Official Secrets Act.

Bodies obliged to make information available and accessible to the public

The Act requires designated "public authorities" to make information they hold available and accessible to the public. These public authorities must also publish details of their procedures for accessing such information.

There are three categories of public authorities specified in the Act.
The first category consists of government ministries, government departments and statutory boards or authorities (whether incorporated or not). This would cover statutory corporations performing quasi-governmental functions.

The second category of public authorities consists of companies which are either wholly-owned by the Government, or in which the Government has at least 51% shareholding, and any subsidiary of such companies. However, in respect of this second category, the Minister has discretion to issue an Order containing exceptions, modifications or adaptations to the Act as he deems appropriate. An Order of this kind is subject to a "negative resolution".

The third, and final, group of designated public authorities consists of those which the Minister, in exercise of his discretion, declares by Order, to be public authorities. This includes (a) any other company not covered in the second group above; (b) any other entity that provides services of a public nature that are essential to the welfare of the Bahamian society, or in respect of such aspects of the entity's business specified in the Ministerial Order; and (c) any entity which receives government funding on a regular basis.

The most important obligations of a designated public authority are to implement the machinery necessary to facilitate processing of requests for information (including appointing an Information Manager and implementing an internal review process to address grievances by applicants); and to publish and make available to the public the following information:

(a) a description of its functions;

(b) a list of its agencies and departments, the matters handled by each, and their respective locations;

(c) its office hours and those of its agencies and departments;

(d) the identity of its information officer and his business address; and

(e) a statement listing the information available from the authority which it uses to make decisions and recommendations pursuant to its statutory mandate; and its programme setting out the rights, privileges and benefits to which the public may be entitled or, in respect of obligations and penalties to which the public may be subject. This statement and any updates to it must be gazetted.

The preceding information must be published within twelve months of the Act coming into force, or within twelve months of being established in the case of entities brought into existence after the Act comes into force; or within twelve months of an Order being issued declaring an entity to be a public authority.

Administrative Framework for a request

A request for information must be in writing and contain sufficient details to assist the public authority with locating the information. The public authority is obliged to assist an applicant with the preparation of a request if such assistance is needed. An applicant does not have to give a reason for seeking access to information.

An applicant must receive the information in the form in which he requests it unless the form requested would be detrimental to the preservation of the record, inappropriate in view of the record's physical state, or would infringe intellectual property rights subsisting in the information.

Requested information may be supplied in the form of copies of records (documents, audio or visual recordings such as CDs); by arranging for the records to be inspected; or by means of transcript of materials that are not reproducible, or which are in shorthand or codified form.

An applicant may be provided with partial access where a part of the requested information contains exempted information.

As a general rule, an applicant must receive a response within 30 days of submitting the request. There are four possible responses an applicant may receive to his request, namely, that the request –

(i) is accepted and the desired access provided;

(ii) has been denied, with an explanation of the reasons for denial and details of options for review of the decision;

(iii) has been deferred, along with the reason for, and the time period of, the deferment; or

(iv) will require an extension of time for processing (which extension cannot exceed an additional 30 day period).

The Act sets out permissible grounds for denial and deferment.
A public authority has discretion to charge a fee for reproducing and communicating information.

Information which is exempted from disclosure under the Act

First of all, the Act excludes completely from its scope, information held by:-

- the prudential regulators of financial services, i.e. the Central Bank, the Securities Commission and the Insurance Commission

- judicial functions of a court or holder of judicial office
- the strategic or operational intelligence gathering activities of the Police, Defence Force, Customs Department, Immigration and the Financial Intelligence Unit; and
- private holdings of the National Archives where the arrangements under which the holdings have been transferred to that department prohibit disclosure as contemplated by the Act.

The Minister under the Act has power to add to this list of exclusions.

In addition to the exclusions above, the agency to which a request to supply information has been made has absolute discretion to prohibit the release of the information (or parts of such information) in the following circumstances:-

- where disclosure would prejudice the security, defence or international relations of The Bahamas;
- where the requested information contains confidential information from a foreign Government or international organisation;
- if the disclosure would or would reasonably be expected to endanger a person's life or safety; affect a trial/adjudication, investigations or prosecution for a breach of the law; reveal the identity of a confidential informant; reveal techniques or methods for law enforcement investigations; facilitate escape from detention; or jeopardise the security of a prison;
- where records are subject to legal or parliamentary privilege or where disclosure would constitute a breach of confidence or contempt of court;
- where the records constitute deliberations or consultations arising in the course of Cabinet or one of its committees; or are consultations/deliberations between the Prime Minister and the Governor-General; or disclosure would prejudice the maintenance of the convention of collective responsibility of Ministers.

Further, an agency to which a request is made may prohibit the release of such information on "public interest" grounds, a sort of conditional discretion. The definition of what will constitute "public interest" has been left to be determined by Regulations.

No Regulations have promulgated thus far under the Act. There is actually a two-tier approach to the public interest test exemptions. As a first step, the Minister with portfolio responsibility for the Act will issue Regulations setting out what the public interest test will consist of. Thereafter, in each individual case where information which is subject to the test is being sought, a determination, applying the public interest test, will have to be

made on whether or not the information should be exempted from disclosure. The circumstances in which access may be denied on "public interest" grounds are as follows:

- where release of the record requested could be expected to have an adverse effect on the economy or the Government's ability to manage it;

- records that are opinions, advice or recommendations prepared for Cabinet or one of its committees;

- where disclosure would likely inhibit free and frank exchange of views for the purposes of deliberations (as it relates to the effective conduct of public affairs);

- where the record is legal advice given by the Attorney General or on his behalf;

- where disclosure would otherwise prejudice the effective conduct of public affairs;

- where disclosure would reveal trade or commercial secrets;

- where disclosure might result in destruction, damage to or interference with conservation and preservation of heritage efforts;

- where the information sought is personal information about another person; and

- where the disclosure would endanger the health or safety of an individual.

Certificates of exemption

The relevant Minister may issue a certificate of exemption in respect of information sought to which access is denied –

- where disclosure would prejudice the security, defence or international relations of The Bahamas;

- where the requested information contains confidential information from a foreign government or international organisation;

- if the disclosure would or would reasonably be expected to endanger a person's life or safety; affect a trial/adjudication, investigations or prosecution for a breach of the law; reveal the identity of a confidential informant; reveal techniques or methods for law enforcement investigations; facilitate escape from detention or jeopardise the security of a prison;

- where disclosure would likely inhibit free and frank exchange of views for the purposes of deliberations (as it relates to the effective conduct of public affairs);

- where the record is legal advice given by the Attorney General or on his behalf;

- where disclosure would otherwise prejudice the effective conduct of public affairs;

- where disclosure might result in destruction, damage to or interference with conservation and preservation of heritage efforts; and

- where disclosure would prejudice the maintenance of the convention of collective responsibility of Ministers.

Any certificate issued in respect of a denial of a request on the final ground immediately above, i.e. that disclosure would prejudice the maintenance of the convention on collective responsibility of Ministers, is not open to question or challenge before any court or otherwise, and acts as a complete veto by the Minister with responsibility for the Act.

Similarly, the Minister with responsibility for the Act may prohibit the Information Commissioner from accessing any information during an investigation by the Commissioner where the Minister feels that it is in the public's interest to prevent the Commissioner's access. A prohibition in this case is also an absolute veto which, under the Act, cannot be questioned by any court or otherwise challenged.

The Act does enable an applicant to request a review of, or appeal a denial of access except where the denial was on the grounds that the collective responsibility of Ministers may be prejudiced by the disclosure.

Two main observations are worth making in relation to exemptions generally.

The first relates to the need to reconcile the apparent conflict between the provisions of the Act dealing with personal information and the regime for protection of personal information under the Data Protection (Privacy of Personal Information) Act (DPA).

Currently, under the Act, a public authority has discretion whether to disclose to a third party, personal information (undefined) on a living or a dead person, where the authority determines that the disclosure is "reasonable" and the balance of public interest factors in favour of disclosure prevail. This position is contrary to the DPA, as well as a deviation from the international standards on data protection principles as regard living persons. Sections 6, 17 and 22 of the DPA set the framework for disclosure of personal information pertaining to living persons in accordance with international standards.

With respect to the provisions in Part IV of the Act, which addresses amendments and annotations to personal information, it should be noted that the DPA also provides a procedure for affected persons to have erroneous or outdated information corrected. So long as the procedure in Part IV of the Act complements the procedure under the DPA, no issue will arise. As previously noted, the Act, unlike the DPA, seeks to address the

disclosure and handling of personal information for dead persons as well. This consideration justifies the inclusion of provisions dealing with personal information in the Act.

However, to avoid confusion between the regime under the DPA and the proposed regime under the Act, a reconciliation of the relevant sections in the two laws is necessary to ensure that no unintended dilution in the international standard for data protection occurs in the overall regime of The Bahamas regime.

The second main observation on exempted information relates to the absence of an exemption for audits, examinations, test and negotiations. These exemptions exist in many other Freedom of Information laws.

The Regulatory Structure for Freedom of Information

The regulatory structure under the Act establishes the Office of Information Commissioner. The Information Commissioner, who is the same person as the Data Protection Commissioner, is answerable to Parliament.
Public authorities are required to submit periodic reports to the Commissioner on their activities under the Act.

Aggrieved applicants may also appeal an adverse decision, in response to a request for information, to the Information Commissioner. However the Commissioner has no power to nullify a certificate of exemption issued by a Minister, where the information exempted relates to the defence, security and international relations of The Bahamas; law enforcement; heritage sites; or, where such information is exempted on the grounds that it may be prejudicial to the effective conduct of public affairs to the maintenance of the convention of collective responsibility of Ministers.

The Information Commissioner is endowed with powers to investigate, and to compel production of evidence and testimony of witnesses. The Act provides for a right of appeal against the Commissioner's decision to the Supreme Court by means of judicial review. Decisions and orders of the Commissioner are binding and enforceable under the Supreme Court's rules for contempt.

Whistle Blowing

The Act provides "legal" protection for whistle blowers where the whistle blowing discloses wrongdoing (commission of a criminal offence; failure to comply with a legal obligation; miscarriage of justice or corruption, dishonesty, or serious maladministration) has occurred. The regime in the Act is weak by any standards as it only declares that there should be no retaliation against a whistleblower. It does not impose penalties for such action, nor does it provide a mechanism or tangible protections for a whistle blower that may be subject to sanctions, in violation of the provision in the Act.

Protection from liability for defamation, breach of confidence and intellectual property rights violations.

The Act is not to be construed as authorizing the publication of information (i) containing defamatory matter, (ii) in breach of confidence, or (iii) in violation of intellectual property rights. In circumstances where such information may have been released unintentionally, the entity or person releasing the information on behalf of the Government and the person who would have supplied the information to Government initially, are protected from action. Additionally, the person receiving such information is expressly prohibited from its further publication.

Conclusion

An effective and meaningful framework (laws, policies, processes, institutions and infrastructure) for access to government information is a strong indicator of progressive democracy. However, effectiveness can only be realized through a conducive machinery that facilitates the objectives of the law and that takes due account of the national environment. The journey to creating that framework must involve the stakeholders that will be responsible for its implementation, primarily the civil servants. Freedom of information is not simply about access by the media, but encompasses the notion that citizens can contribute to all facets of national development by having available to them, information that can stimulate ideas and discussions on issues of concern to them and also assist them in understanding how their Government works. Traditional notions of Government meant that often its machinery was not structured to accommodate such democratic involvement. This machinery must therefore undergo adjustments and re-engineering to be able to operate in the new open governance framework; and each country is likely to have different experiences with this journey. More importantly very few countries, if any, seek to do it overnight. Yes, the principles for access to information are fairly universal, but to be effective they must be appropriately implemented and adequately contextual.

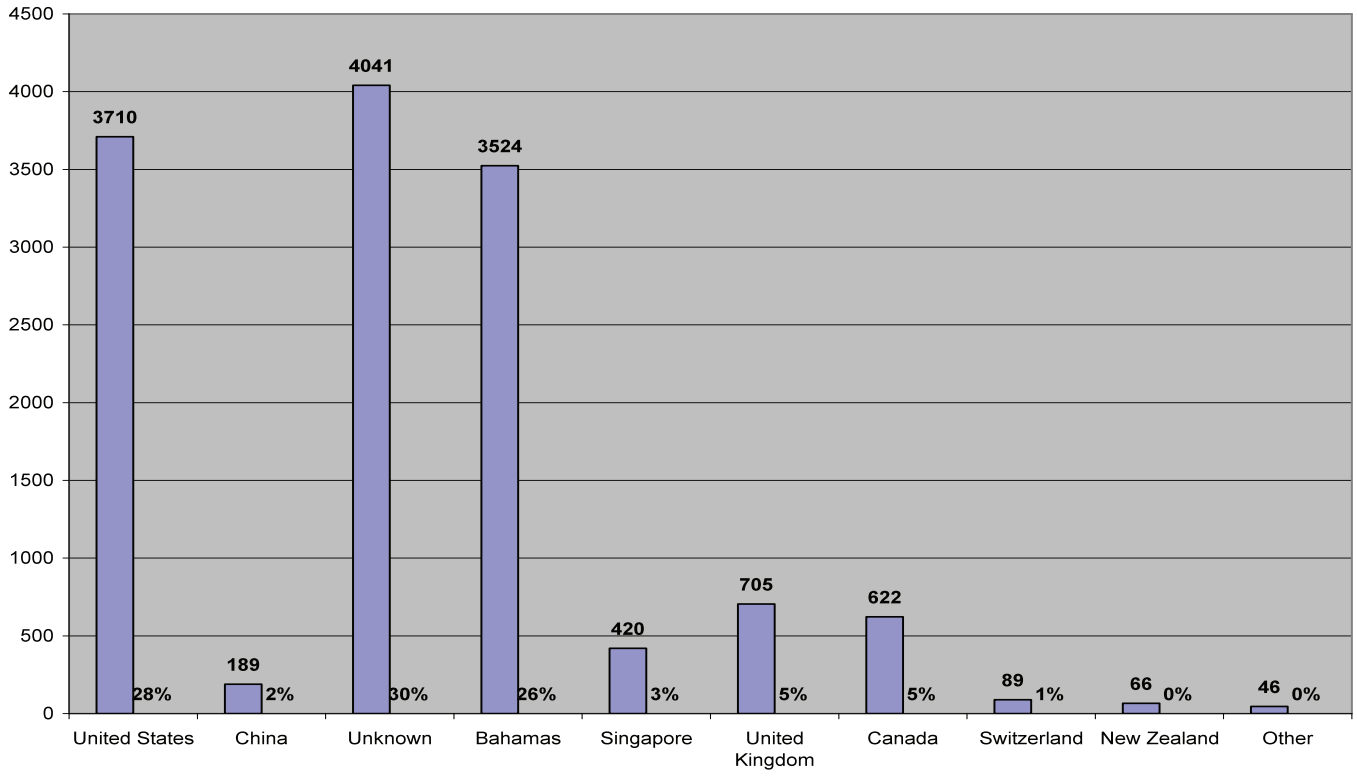
Rowena G. Bethel is a member of the United Nations Committee of Experts on Public Administration (CEPA), which operates under the auspices of the UN Department of Economic and Social Affairs (UNDESA). She is a qualified barrister-at-law of the Middle Temple Inn of Court, England and a member of The Bahamas Bar. She holds a LL.B degree from Leicester University, UK and a Master of Laws degree in Information Technology and Telecommunications law from the University of Strathclyde, UK. She was the architect of the suite of enabling e-commerce legislation passed in 2003 which include the Electronic Communications and Transactions Act, the Computer Misuse Act and the Data Protection (Privacy of Personal Information) Act; and the legislative framework for international tax cooperation by The Bahamas. She is a former Legal Advisor to the Ministry of Finance.rowenabethel@gmail.com

Appendix 2

REPORT ON WEBSITE STATISTICS

As noted previously a new format for website statistics is now available. The period covered by the below information relates to the months of January and February, 2012, then October, 2012 through January, 2013. The figures show that the site is being accessed by a variety of countries who seek to know more about the data protection regime in The Bahamas.

	Country	No. of Hits	Visitors	%
1	United States	3,710	144	28
2	China	189	92	2
3	Unknown	4,041	91	30
4	Bahamas	3,524	34	26
5	Singapore	420	20	3
6	United Kingdom	705	10	5
7	Canada	622	8	5
8	Switzerland	89	1	1
9	New Zealand	66	1	-
10	Others	46	11	-
	Total	**13,412**	**412**	**100**



Appendix 3

SCHEDULE OF VISITS AND/OR PRESENTATIONS

Date	Agency/Institution	Number of Participants
Jan. 03	St. Anne's School	63
Mar. 13	Dept. of Public Service	41
Mar. 27	C.I. Gibson Sr. High School	63
May 26	Church of Christ Women's Group	13
Aug. 29	Doris Johnson Sr. High School	75
Nov. 09	Faith United Men's Group	53

Appendix 4

TIP OF THE MONTH

During the year the following topics were promoted through our "Tip of the Month" feature:-

January	Facebook – A Fresh Start in 2012.
February	Using a Driver's Licence for Identification Purposes.
March	Disclosure of Personal Data in Certain Cases.
April	Choosing a Good Password.
May	Ten Things HR Professionals Need to Know About Privacy (Data Protection).
June	Protect Yourself Against Hackers.
July	Employers Responsibilities under the Data Protection (Privacy of Personal Information) Act, 2003 (DPA).
August	It's Vacation Time Again!
September	Back to School Safety Message.
October	Beware of Job Hunting Scams!
November	Data Protection and Charitable Organizations.
December	Christmas Privacy Tips.

The focus has been on protecting the privacy rights of individuals in an environment where the use of social media is fast out-pacing the more traditional means of communication .

Appendix 5

EDUCATION CORNER

Language and culture are changing daily in the world of Data Protection. Here are a few terms which have come alive in recent times:-

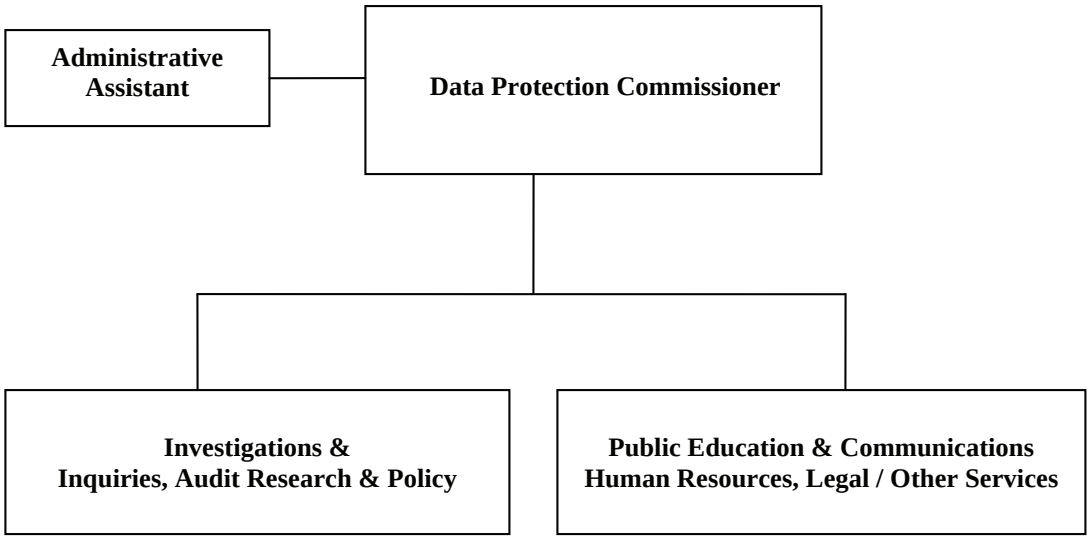
TERMS	MEANING/IMPLICATION
BLAGGING	The practice of pretending to be someone else in order to get personal information about them, for example from their bank or their doctor.
BOTNET	A botnet is a collection of internet-connected computers whose security defenses have been breached and control ceded to a 3rd party. Each such compromised device known as a "bot" is created when a computer is presented by software from a malware distribution, otherwise known as "malicious software." The controller of a botnet is able to direct the activities of these compromised computers through communication channels formed by standard-based network protocols such as IRC (Internet Relay Chat) and HTTP (Hypertext Transfer Protocol).
CATFISHING	To pretend to be someone you're not online by posting false information, such as someone else's pictures, on social media sites usually with the intention of getting someone to fall in love with you. People who "catfish" keep others on their toes but can also use the method to inject meaning into their own lives.
CLOUD COMPUTING	A model for delivering information technology services in which resources are retrieved from the internet through web-based tools and applications rather than a direct connection to a server. Data and software packages are stored in servers. However, cloud computing structure allows access to information as long as an electronic device has access to the web. This type of system allows employees to work remotely.
DATA EXPLOSION	The rapid increase in the amount of published information or data and the affects of this abundance. As the amount of available data grows, the problem of managing the

	information becomes more difficult which can lead to data overload.
SNAPCHAT	A photo messaging application; users can take photos, record videos and text and drawings, and send them to a controlled list of participants. Users set a time limit for how long recipients can view their photo, up to 10 seconds, after which it will be deleted from the recipient's device and the company's servers. (Somewhat like "Mission Impossible" self-destruct after use!)

Appendix 6

ORGANIZATION BY FUNCTIONS

The staff in the ODPC is comprised of the Commissioner and his Secretary (described as an "Administrative Assistant" in the below chart). The chart, however, depicts the functions of the office which are now within the purview of the Commissioner, but which may revolve into job positions/units with the growth of the activities of the ODPC. It should be noted that the ODPC is located within the premises of the Ministry of Finance and is able to call on the Legal Unit of the Ministry for advice and assistance in case of need. No staff adjustments are planned at this time.



A synopsis of the various activities and/or comments in each work category is given below:

Investigations and Inquiries

- Investigating complaints received from individuals under Section 15 of the DPA.
- Establishing whether individuals have had their privacy rights violated.
- Determining whether individuals have been afforded their rights to access to their personal information.
- Where privacy rights have been violated, seek to provide redress and to ensure violations do not recur.
- Mediation and conciliation, with a view to corrective action, if necessary, are the preferred approaches to complaint solving.

- The Commissioner has the power to issue enforcement notices to compel violators to comply with the provisions of the DPA.
- There is provision under Section 24 of the Act for leave to appeal to the Court against the prohibition specified in the Notice within 21 days from the service of Notice.
- The Commissioner's office will be receptive to all privacy complaints, Section 15 (2) (a). However frivolous or vexatious complaints will be discouraged.

Audit Research & Policy

- Here we will assess how well organizations comply with the provisions and spirit of the DPA.
- Compliance reviews of the function and or work of a Data Controller or a Data Processor is also the concern of this area, and the application of the Act outlined in Section 4 of the DPA.
- The Commissioner will receive, analyze and provide comments and recommendations on Data Protection issues affecting The Bahamas.
- He will also seek to ensure that privacy risks associated with specific programs and services are properly identified and that appropriate measures are taken to mitigate these risks.
- Develop a center of expertise on emerging Privacy/Data protection issues at home and abroad.
- Research trends, monitor Legislative and regulatory initiatives and provide analysis on key issues, including policies and positions that advance the position of the Privacy rights of personal information.
- Identify Legislation, new programs and emerging technologies that raise privacy concerns, providing strategic advice and policy options.
- Draft discussion and/or position papers for public consumption on issues affecting Privacy; and personal briefing material for public speeches etc.

Public Education & Communication

- Promote the observance of good practice by Data Controllers within the requirements of the Act.
- Provide information to the public about the Legislation and how it works, and about relevant matters.
- Issue codes of practice for guidance as to good practice about Data Protection.
- Encourage the preparation and dissemination of Data Protection codes of practice by trade associations; consider codes submitted for review and ensure appropriate consultation, providing an opinion on the codes as to good practice.
- Discharge various functions relating to or arising from international obligations of The Bahamas, as regards Data Protection (privacy) issues.
- Plans, and implements a number of public education and communications, activities, including speaking engagements and special events, media relations, advertising, the production and dissemination of promotional and educational

material. Clearly all of the above will not fall into place immediately, but it is anticipated that the framework will evolve over time.

Human Resources – Legal & Other Services

- The message must go out to Human Resource Management Personnel that they are responsible for performing Data Protection functions either as a Data Controller or a Data Processor for the purposes of the Act.
- In particular, the Head of a Government Agency is deemed to be Data Controller or as the case may be, a Data Processor under Section 3 of the Act.
- Legal matters under the Act will be referred to the Legal Advisor in the Ministry of Finance.
- Other services, notably advice on finance, information technology and general administration will be sought from development partners within the Ministry of Finance.

FINANCIAL STATEMENTS

Receipts and Payments for the period January 1st, 2012 to December 31st, 2012

(Expressed in Bahamian Dollars)

Receipts	**2012**	**2011**
Contribution provided via the Ministry of Finance (Note 1)	143,253	125,058
Total Receipts		**125,058**
Payments		
Salary & Allowances (Note 2)	133,900	101,400
Awareness Campaign		14,869
Transport, Travel & Subsistence	5,013	1,940
Training & Related Costs	500	3,424
Office & Computer Expenses	498	834
Miscellaneous Expenditure (Note 3)	3,342	2,591
Total Payments	**$143,253**	**$ 125,058**

Notes:-

1. **Contribution provided via the Ministry of Finance.** The Commissioner does not operate an independent accounting function. All expenses of the Office are met from within the resources of the Ministry of Finance. Consequently the expenses detailed in the above financial statement are of **notional value only.**

2. **Salaries & Allowances.**

   (a) The figure at note (2) includes a gratuity payment to the Commissioner at the end of a previous contract which expired in October, 2012. It also accounts for one staff member directly assigned to the Office of the Data Protection Commissioner.

   (b) Staff other than the Commissioner, are established public officers. Presently the complement consists of the Commissioner and Secretary.

3. Includes the cost of car refurbishment following a road accident.

OFFICE OF THE
DATA
PROTECTION COMMISSIONER

CONTACTS

First Floor
Cecil Wallace-Whitfield Centre
West Bay Street
P. O. Box N-3017
Nassau, Bahamas
Tel.: (242) 702-1552/ 702-1534
Telefax: (242) 327-7501
E-mail: dataprotection@bahamas.gov.bs

Designed & printed by Government Printing Department