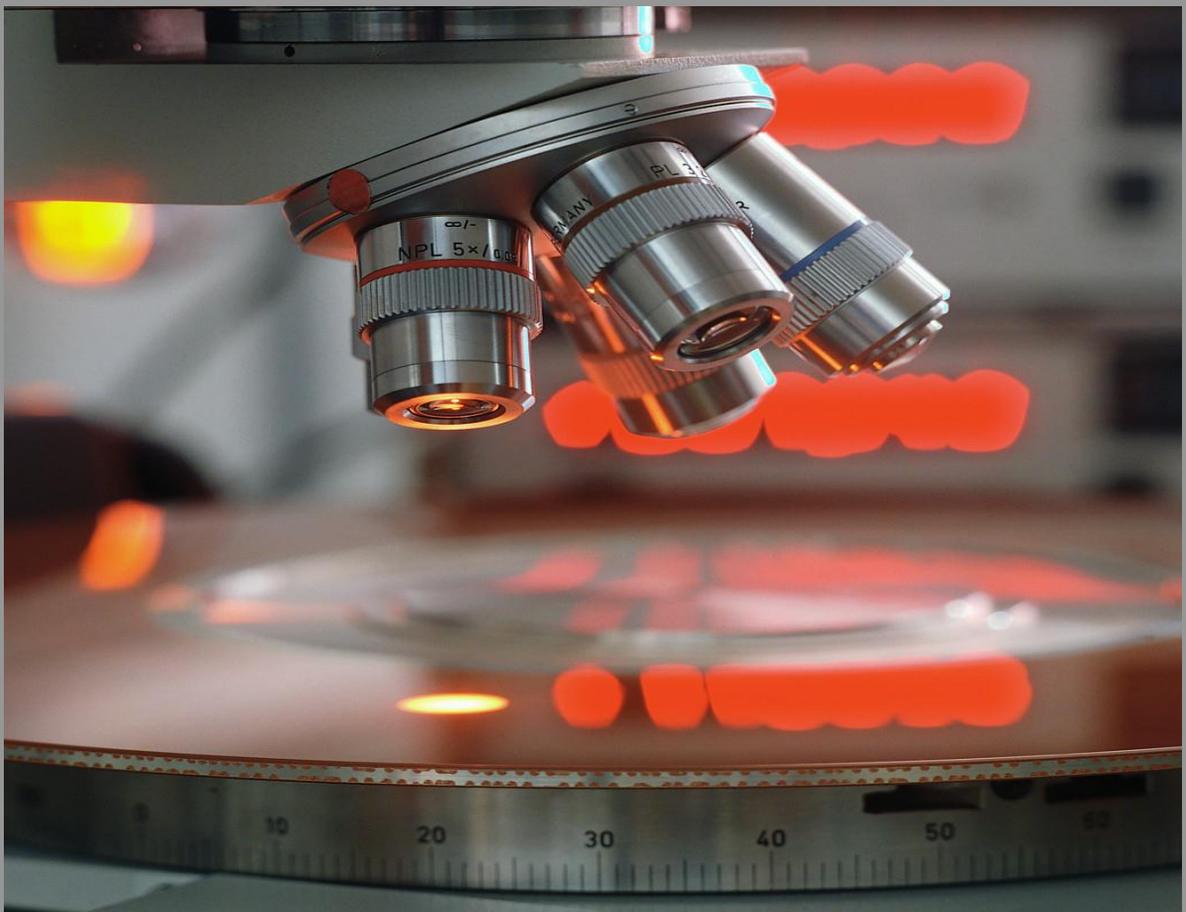




OFFICE OF THE
DATA
PROTECTION COMMISSIONER



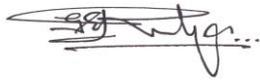
Annual Report 2011

**The Honorable Hubert A. Ingraham
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 fifth Annual Report on the activities of the Office of the Data Protection Commissioner for the reporting year ended December 31st 2011.

Yours faithfully,

A handwritten signature in black ink, appearing to read "George E. Rodgers", with a horizontal line drawn underneath it.

George E. Rodgers
Data Protection Commissioner

February 2012

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.

“But what I want to ensure and reassure the public is we are concerned about your safety, your security, and your privacy. Let’s work together in partnership to ensure that we can have the best way forward.” (John Pistole).

LIST OF ABBREVIATIONS

APPS	- Applications (for Computers etc.)
BGOL	- Bahamas Government Online
CARTAC	- Caribbean Regional Technical Assistance Centre
CCTV	- Closed Circuit Television
CMA	- Computer Misuse Act, 2003
DPA	- Data Protection (Privacy of Personal Information) Act, 2003
EU	- European Union
FOIA	- Freedom of Information Act
IFAI	- Instituto Federal de Acceso a la Informacion y Protection de Datos (Mexican Federal Institute for Access to Information and Data Protection)
IFC	- International Finance Corporation
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.....	6
Commissioner’s Statement.....	7
Selected Terminology in the Data Protection Act.....	9
Data Protection - A Quick Guide.....	10
Data Protection Principles and Hints of their Usage.....	11
The Commissioner at Work	14
Duties of the Commissioner.....	17
Powers of the Commissioner.....	18
Appendix 1 Website Statistics.....	19
Appendix 2 Identity Theft	20
Appendix 3 Schedule of Agency Visits and/or Presentations	23
Appendix 4 Tip of the Month	24
Appendix 5 Organization by Functions.....	25
Appendix 6 Focus on the Computer Misuse Act.....	28
Appendix 7 Financial Statements.....	30
Contacts – Back Page	

FOREWORD

This is my fifth report as Data Protection Commissioner for the Bahamas. It covers the year 2011. The Data Protection (Privacy of Personal Information) Act, 2003, (DPA) has been in force since 2nd April, 2007 and is now fully operational except for the provision of Section 31 (2) which comes to maturity in early April 2012. This section states 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 take this opportunity to encourage all stakeholders to ensure that personal data files in their care are fully updated and/or purged to promote good data practices as mandated by the DPA.

2011 has been another year which has seen the privacy rights of individuals impacted (both positively and negatively) by the common use of the internet as a means of communication through Twitter, Blogs, Facebook etc. The Office of the Data Protection Commissioner (ODPC) continues to monitor how these communication means affect our citizenry and offer suggestions on how to protect their privacy through our “Tip of the Month” feature.

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 resides; the continuous use of best practices in the field of data protection is one of many ways of fulfilling our mandate.

COMMISSIONER'S STATEMENT

“Time goes quickly by” as already this is my fifth year and report since becoming the Data Protection Commissioner. I am pleased to present Annual report 2011 highlighting the activities of the year.



Promoting and protecting the privacy rights of individuals in our society is at the core of my mandate as Data Protection Commissioner. This task remains challenging as we continue to operate with limited resources. Now-a-days one of the key indicators of promotion is an effective Website which regrettably was not available to us during the last six months of 2011. Consequently, **Appendix 1** only records the statistical activity for the first half of the year. During this period, a total of 2687 hits were recorded indicating that interest in the benefits of data protection is relatively steady.

One theme that resonated throughout 2011 was the tendency of security authorities and practitioners in the commercial sector to collect more personal information than was needed to carry out their duties or conduct their businesses effectively. During the coming months I intend to focus on this and the emergence of identity theft in our local communities. See **Appendix 2** for more information on the meaning and threats associated with identity theft.

It is worthwhile to note that last October, the Government of The Bahamas introduced to Parliament for the first time a Freedom of Information Act, (FOIA). Freedom of Information is closely aligned with Data Protection of Personal Information (and the DPA) for which I have primary responsibility.

There must be a “balance” between the citizens’ right to public information as proffered by the FOIA and the individual’s right to privacy (data protection) under the DPA, as one should not be sacrificed at the expense of the other.

Canada, the United Kingdom (UK), Australia (to name a few) have seen the wisdom in placing both data protection and freedom of information under one umbrella known as “The Office of the Information Commissioner” with an appointed “Information Commissioner” responsible for each arm of this vital initiative. The Bahamas has an opportunity to make this adjustment almost immediately. FOIA is expected to come on stream sometime in 2012.

Once again complaints and/or queries have been few with five (5) complaints and thirty (30) queries being received. This compares with six (6) complaints and thirty two (32) queries in 2010. During 2011, I made sixteen (16) visits/road trips making contact with

three hundred and ninety four (394) individuals in the process, (prior year nineteen (19) visits and three hundred and forty eight (348) individuals). See promoting public awareness (page 14) which highlights our efforts to address this area.

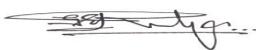
The 33rd International Conference of Data Protection Commissioners was held in Mexico City, Mexico during the first week of November 2011. It was hosted by The Mexican Data Protection Authority, “Instituto Federal de Acceso a la Información y Protección de Datos” (IFAI) at the Hilton Mexico City Reforma. There were several parallel events which together attracted over 620 participants from 88 countries around the world:-

No.	Date	Event	Theme
1	31 Nov.	The Public Voice Meeting	“Privacy is Freedom”
2	Nov. 1	OECD Conference	“Current developments in Privacy Frameworks: Toward Global Interoperability”
3	Nov 1	Privacy by Re-Design	“A Transformative Process”
4	Nov 2 & 3	Conference 33	“Privacy: The Global Age”

I was privileged to represent The Bahamas at events 2 and 4. These conferences provide a forum for discussion and offer suggestions on the way forward in the ever changing realm of data protection. Details of the resolutions passed and reproduction of many of the discussion papers may be found at www.privacyconference2011.org

As a data protection authority, the ODPC and The Bahamas are pleased 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 under active consideration. The enactment of the DPA overcame the first hurdle. Secondly, our initial attempt to produce a set of Regulations arising from the DPA requires more research and we shall continue our efforts in this regard. Thirdly, we continue to encourage our community to take advantage of our facilities to enhance our Case Management Skills.

Finally, I am obliged to thank the Acting Financial Secretary Mr. Ehurd Cunningham for his continued support to the work of the ODPC. 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, 2012

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

Arguably, one of the most important aspects of our work is promoting the general awareness of data protection both to the public and to organizations operating in The Bahamas. Consequently, the awareness campaign that started last year continued well into 2011 with Public Service Announcements (PSAs) via Radio and Television dealing with aspects of data protection relative to the meaning and application of data protection principles. This will be enhanced with the introduction of a “Facebook” page and a “Twitter” account by June of 2012, to take advantage of some of the modern means of communication beyond the basic Website.

A focus must now be given to several key issues such as:

- how to make, and how to deal with a subject access request
- personnel issues, including the provision of employment references and data retention
- social Networking sites and internet blogs;
- the inclusion of fair processing statements on data collection forms
- internet security and safety, particularly in respect of children’s privacy;
- publication of photographs and personal information on the internet.

A broader awareness of the above topics should yield an increase in both formal complaints and general enquiries. During the year we processed five (5) formal complaints and thirty (30) queries via telephone and e-mail, compared with six (6) complaints and thirty two (32) queries in 2010. Of the five (5) complaints recorded:-

- two related to refusals to release personal information on request within the 40 days window, as required by the DPA
- two related to failures to remove questionable and unproven information from staff files
- one referred to the refusal to remove a malicious posting from a social networking site.

Four of these were successfully resolved; one remains under investigation.

While on holiday in July, Commissioner Rodgers and family were privileged to pay a courtesy call on Bahamas Counsel General to New York, Mrs. Rhonda Chipman-Johnson and staff. He took the opportunity to chat with members of the staff who were surprised that the Bahamas had such progressive legislation on its books dealing with data protection.

Promoting Public Education

During 2011 the Commissioner made sixteen (16) road trips/presentations spread among government agencies, schools, banking and civic organizations. Through this medium, direct contact was made with three hundred and ninety four (394) individuals; this compares with nineteen (19) visits and three hundred and forty eight (348) individuals the year before. (See **Appendix 3** for a Schedule of Visits and/or Presentations).

From **Appendix 3** you will note that several trips were made to the Bank of The Bahamas and S. G. Hambros Ltd., where the Commissioner participated in several in-house training exercises with selected employees as part of the training commitment of each institution. The public should know that the Commissioner is available to them both for speaking engagements and/or assisting with training in and compilation of data protection codes and protocols.

Appendix 4 highlighted our “Tip of the Month” feature. Each topic discussed is still available to the public from the “Tip of the Month-Archives” on our Website www.bahamas.gov.bs/dataprotection.

Below is a summary of data statistics over the last five (5) years.

Particulars	2007	2008	2009	2010	2011	Totals
Complaints	1	3	5	6	5	20
Queries	9	20	22	32	30	113
Presentations /Visits	19	25	18	19	16	97
Inter-Actions	229	473	304	348	394	1748
Website Hits (incomplete)	N/A	6314*	N/A	2608	2687	11,609

* Represents the only year when full website statistics were available. All other periods reflected six (6) months figures.

In addition to the above, The Commissioner, was able to visit several Family Islands, including Grand Bahama, Abaco, Exuma, Andros, Cat Island and Bimini. Visits planned to Eleuthera and Long Island were aborted during 2011 due to the passage of Hurricane Irene. These and other Family Islands will be visited in due course.

During several of our road trips, questions arose about the relationships of The Computer Misuse Act to the DPA. **Appendix 6** presents a brief focus of this regard.

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 should come to

fruition in early 2012. 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. It is expected that significant progress toward completion of this project will be made by the end of 2012.

Last year the Commissioner began the process of compiling an initial set of Regulations to supplement the DPA. The assistance of the Office of the Attorney General (OAG) Law Reform Unit was solicited to help in this regard.

We reiterate that prior April 07, 2012 and in accordance with Section 31 (2) of the DPA, relative to the 5 year grace period, all stakeholders should have ensured that personal data files have been updated and/or purged of all unwanted personal information thereby ensuring they are ready to promote good data protection practices.

After all ... "Privacy is 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

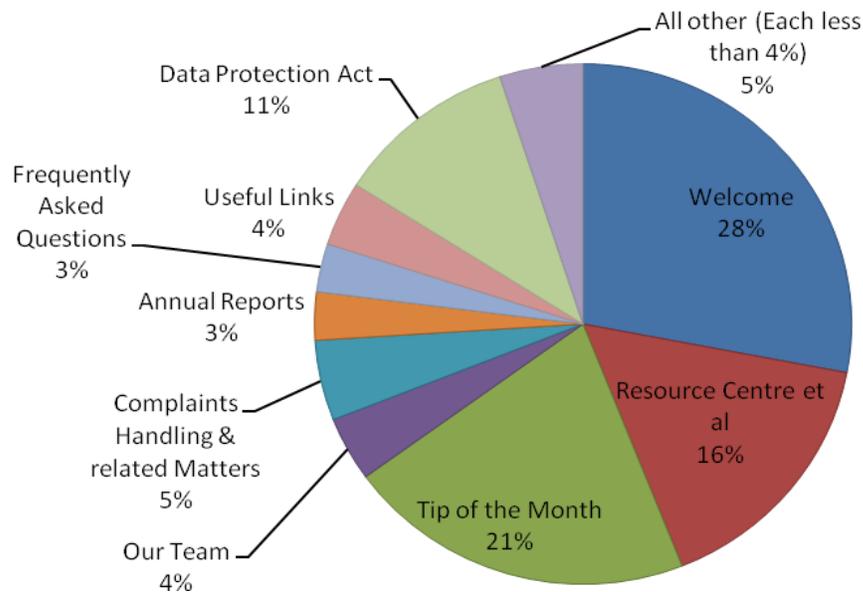
1. ***Enforcement powers****. These include service of information notices (S.18) and enforcement notices (S.16), to enable the Commissioner to investigate and rectify instances of non-compliance with;
 - any of the data protection principles,
 - any other requirements of the DPA.
2. ***Transborder data 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.**

WEBSITE STATISTICS FOR SIX MONTHS JANUARY 01, 2011 – JUNE 30, 2011

As noted previously our website statistics (on the number and subject of “hits”) were unavailable after 30th June 2011. It transpired that the government of The Bahamas introduced a new e-mail portal which merged our website with that of the central government. Consequently, the statistics below only reflect the period noted above.

Area	No. of Hits	Percentage
Welcome	739	28
Resource Centre et al	437	16
Tip of the Month	574	21
Our Team	98	04
Complaints Handling & Related Matters	144	05
Annual Reports	78	03
Frequently Asked Questions	91	03
Useful Links	70	04
Data Protection Act	310	11
All other (Each less than 4 %)	146	05
Total	2687	100



IDENTITY THEFT

What it is and what you can do about it?

Progress can be costly. And while recent developments in the telecommunication and computer processing make it easier for companies and consumers to reach each other, they also scatter your personal information more widely, making life easier for criminals.

Every year, thousands of people are victims of identify theft, made easier by the rapid pace of development.

Identify thief is the unauthorized collection and use of your personal information, usually for criminal purposes. Such information as your name, date of birth, address, credit card, National Insurance Number and other personal identification numbers can be used to open credit card and bank accounts, redirect mail, establish cellular phone service, rent vehicles, equipment, or accommodation and even secure employment.

If this happens you could be left with the bills, charges, bad cheques and an excruciating headache.

How to fight Identify Theft?

- Minimize the risk. Be careful about sharing personal information or letting it circulate freely.
- When you are asked to provide personal information, ask how it will be used, why it is needed, who will be sharing it and how it will be safeguarded.
- Give out no more than the minimum, and carry the least possible with you.
- Be particularly careful about your National Insurance Number, it is an important key to your identity.
- Don't give your credit card number on the telephone, by electronic mail, or to a voice mailbox, unless you know the person with whom you're communicating or you initiate the communication yourself, and you know that the communication channel is secure.
- Take advantage of technologies that enhance your security and privacy when you use the Internet, such as digital signatures, data encryption, and "anonymizing" services.

- Pay attention to your billing cycle. If credit card or utility bills fail to arrive, contact the companies to ensure that they have not been illicitly redirected.
- Notify creditors immediately if your identification or credit cards are lost or stolen.
- Ask that your accounts require passwords before any inquiries or changes can be made, whenever possible.
- Choose difficult passwords - not your mother's maiden name. Memorise them, change them often. *Don't* write them down and leave them in your wallet, or some equally obvious place.
- Key personal identification numbers privately when you use direct purchase terminals, bank machines, or telephones.
- Find out if your cardholder agreement offers protection from credit card fraud; you may be able to avoid taking on the identity thief's debts.
- Be careful what you throw out. Bum or shred personal information such as statements, credit card offers, receipts, insurance forms, etc. Insist that businesses you deal with do the same.

Are you a victim of identity theft?

- Report the crime to the police *immediately*. Ask for a copy of the police report so that you can provide proof of the theft to the organizations that you will have to contact later.
- Take steps to undo the damage.
- Document the steps you take and the expenses you incur to clear your name and re-establish your credit.
- Cancel your credit cards and get new ones issued. Ask the creditors about accounts tampered with or open fraudulently in your name.
- Close your bank account and open new ones. Insist on password only access to them.
- Get new bank machine and telephone calling cards, with new passwords or personal identification numbers.
- In the case of passport theft, advise the Passport Office.
- Advise your telephone, cable, and utilities that someone using your name could try to open new accounts fraudulently.
- Get a new driver's licence.

If you suspect that someone has been using your NIB number to get a job, or that your ID information has been compromised in some other way, be sure to follow up and get to the bottom of the problem to find out what is really going on.

Putting everything in perspective, you almost need a new life if you become a victim of identity theft.

So guard your identity to the utmost to avoid the potential problems which can be avoided by being very careful about your personal information.

Adopted & Condensed. Courtesy of the Privacy Commissioner of Canada

SCHEDULE OF VISITS AND/OR PRESENTATIONS

Date	Agency/Institution	Number of Participants
Jan. 26	Dept. of Social Services	48
Feb. 03	Bahamas Development Bank's Conference on its future Sustainability	35
Feb. 08	Association of Justices of the Peace	48
Mar. 08	Rotary Club of Nassau	26
May 06	SG Hambros Bank & Trust (Bahamas) Ltd.	31
June 16	SG Hambros Bank & Trust (Bahamas) Ltd.	23
Sept. 13 & 14	Bank of The Bahamas Training Dept.	23
Sept. 26 & 27	Bank of The Bahamas Training Dept.	24
October 25	R.M. Bailey Senior High School	5
October 26	Bank of The Bahamas Training Dept.	10
October 27	D.W. Davis Jr. High School	56
Nov. 16	Jordan Prince Williams School	52
Nov. 23	Queens College	12
Nov. 24	St. John's College	01
	TOTAL	394

TIP OF THE MONTH

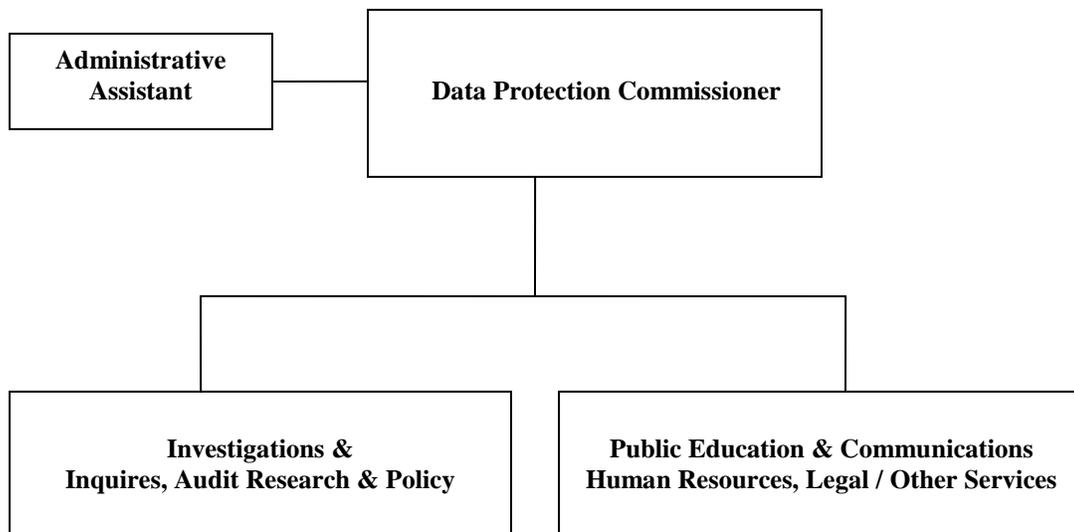
During the year the following topics were promoted through our “Tip of the Month” feature:-

January	Fraud Prevention in Banking.
February	Complain to the Data Protection Commissioner
March	Are you smarter than your smart phone?
April	Spring clean your online privacy.
May	Defend yourself against Identity Theft.
June	Making an Access Request.
July	Tips for Social Networking.
August	Think before you Click!
September	Back to School and Cyber Bullying.
October	Taking Fingerprints in Schools.
November	Six things that make Privacy Work.
December	Protect your Privacy this Christmas.

The focus has been on protecting the privacy rights of individuals against the variety of fraud by scam artists and the need for exercising care when considering the proliferation of new applications (APPS).

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 Personal 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.

FOCUS ON THE COMPUTER MISUSE ACT

The Computer Misuse Act, 2003 (CMA) accompanied the DPA and the Electronic Communications and Transactions Act (ECTA) as an integral part of the Bahamas Government Online (BGOL) initiative. Both the CMA and the ECTA came into force in June 2003 and the DPA in April 2007. “Together these pieces of legislation provide the modern framework for certainty, clarity and the legal validity for the conduct of affairs using electronic means in, and from, The Bahamas” (Rowena Bethel, former Legal Advisor in the Ministry of Finance).

The CMA provides for six specific offences, relating to unlawful interference with computers and computer systems. It provides an important element in meeting security and data protection (privacy) concerns about conducting business in The Bahamas in an electronic manner.

Offences Under the Computer Misuse Act

1. **Unauthorized Access To Computer Material** – This requires a deliberate intention to access information or programs in a computer, with the knowledge that the access is unauthorized.
2. **Access with Intent to Commit or Facilitate The Commission of an Offence** – The offence is committed if someone uses a computer to gain access to any other computer for the purpose of committing an offence. In this case the initial access may be authorized, however the purpose for the access may be criminal. It is also irrelevant whether or not commission of the intended offence is possible.
3. **Unauthorized Modification of Computer Material** – This requires the deliberate alteration of the contents of a computer knowing that such alteration is unauthorized. The offence applies even if the computer affected was not the one targeted.
4. **Unauthorized Use or Interception of Computer Service** – This is the deliberate act of gaining access to computer knowing that there is no authority for such access, to obtain a computer service whether as computer time, data processing or the storage or retrieval of data. This offence is satisfied either by gaining direct access to the service or by utilising any device for intercepting communications with the result that a service is obtained through a subversion.

5. **Unauthorized Obstruction of Use of Computer** – This covers the deliberate act of interfering with the functioning of a computer to prevent access or effectiveness of the operation of the computer, knowing that such interference is unauthorized.
6. **Unauthorized Disclosure of Access Codes** – This creates an offence where any password, access code, etc. is deliberately released in unauthorized circumstances for the purpose of wrongful gain, illegal activity or knowing that the disclosure is likely to cause wrongful loss to any person.

Enhanced penalties (except for the offence of access with intent to commit an offence) apply in the case where an offence is committed which involves a protected computer, i.e. those involving security, defense or international relations, law enforcement, communications infrastructure, financial services, public utilities, electronic authentication, emergency, essential services, medical services and public transportation.

The CMA applies to any offence so long as the accused was in The Bahamas at the material time or the computer program, or data was in The Bahamas at the material time.

Where damage is occasioned as a result of any offence the penalties imposed by the courts can be further increased. In addition the courts may order the defendant to compensate the victim for damage to any computer, data or program.

The CMA is supplemental to the Penal Code of The Bahamas and is enforceable under the general rules provided thereby.

FINANCIAL STATEMENTS

Receipts and Payments for the period January 1st 2011 to December 31st 2011

(Expressed in Bahamian Dollars)

Receipts

	2011	2010
Contribution provided via the Ministry of Finance (Note 1)	125,058	131,723
<hr style="border-top: 1px dashed black;"/>		
Total Receipts	125,058	\$131,723

Payments

Salary & Allowances (Note 2)	101,400	\$100,900
Awareness Campaign	14,869	22,313
Travel & Subsistence	1,940	836
Training & Related Costs	3,424	4,684
Office & Computer Expenses	834	714
Furniture & Fittings (Note 3)	-	-
Miscellaneous Expenditure	2,591	2,276
<hr style="border-top: 1px dashed black;"/>		
Total Payments	\$125,058	\$ 131,723

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 Commissioner was appointed by the Government initially for a period of three (3) years and this appointment has been extended for a further three (3) years to expire in October 2012. The figure at note (2) reflects the remuneration of the Commissioner and his staff.

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

3. **Furniture & Fittings.** The Commissioner maintains an office at the Ministry of Finance. No Purchases were made during the period under review.



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
www.bahamas.gov.bs/dataprotection