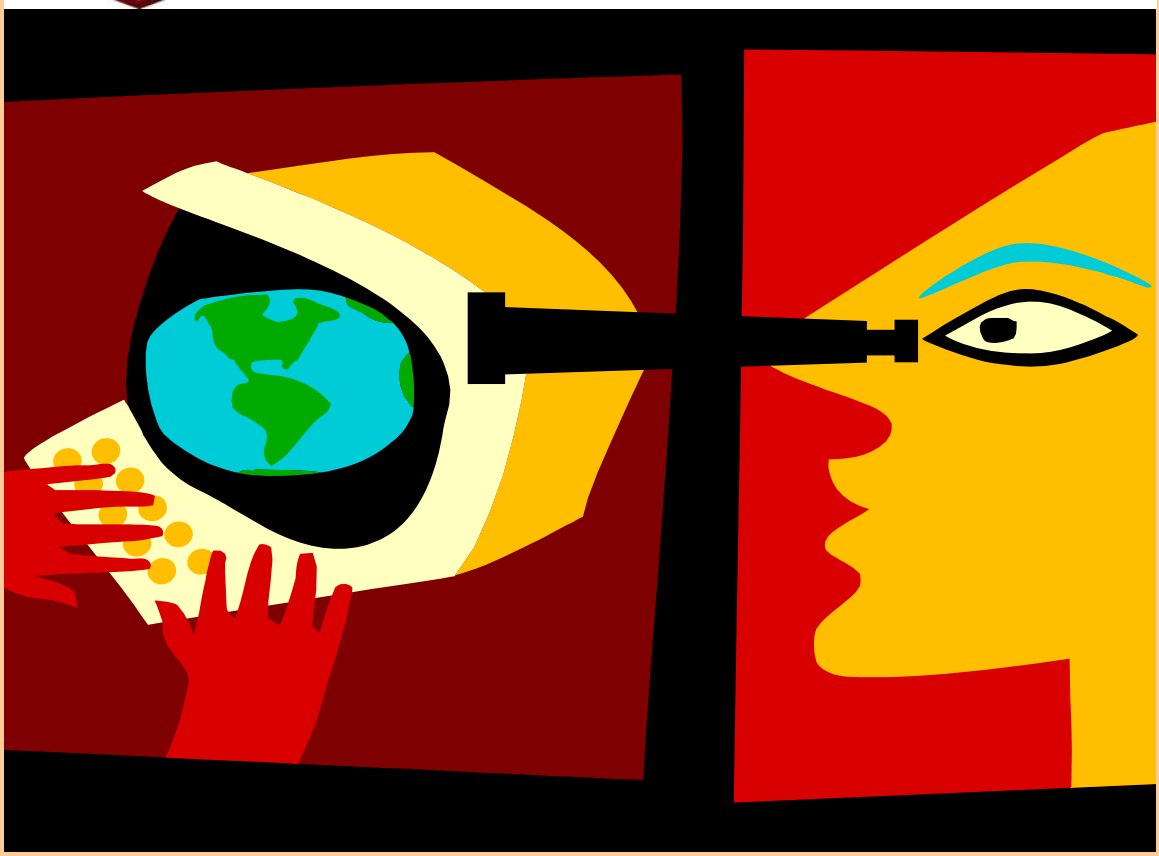
OFFICE OF THE
DATA
PROTECTION COMMISSIONER



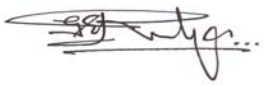
Annual Report 2010

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 fourth Annual Report on the activities of the Office of the Data Protection Commissioner for the reporting year ended December 31st 2010.

Yours faithfully,



George E. Rodgers
Data Protection Commissioner

23rd February, 2011

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.

Remember your privacy ends where the other person's privacy begins. Respect, choice and balance should be the order of the day.

ABBREVIATIONS

BGOL - Bahamas Government Online

CCTV - Closed Circuit Television

DPA - Data Protection Act

EU - European Union

FOI - Freedom of Information

ILITA - Israeli Law Information and Technology Authority

OAG - Office of the Attorney General

ODPC - Office of the Data Protection Commissioner

OECD - Organization for Economic Cooperation and Development

PSAs - Public Service Announcements

RFP - Request for Proposal

TIEAs - Tax Information Exchange Agreements

UN - United Nations

CONTENTS

FOREWORD

The year 2010 represents the fourth year of my appointment as the Data Protection Commissioner for The Bahamas.

We live in an information age where the need to protect our personal information is becoming more acute each day. Thus the enactment of The Data Protection (Privacy of Personal Information) Act, 2003, (DPA) and the establishment of the Office of the Data Protection Commissioner (ODPC) in late October 2006 were truly significant steps in the right direction. The DPA came into force on April 2nd, 2007 and was accompanied in 2003 by the Computer Misuse Act and the Electronic Communications and Transactions Act. Together they augment the mandate of the DPA which gives citizens important rights including the right to know what information is held about them and the right to correct information that is wrong. The DPA helps to protect the interest of individuals by making it an obligation of both the private and the public sectors to manage the personal information they hold in an appropriate way that is consistent with the rights of the data subject as provided by law.

As a Corporation sole, the Commissioner is independent in the performance of his duties. By law he is appointed in writing by the Governor General on the advice of the Prime Minister after consultation with the Leader of the Opposition. The Commissioner has 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.

The Bahamas is part of the global arena and we are inextricably linked to and affected by the advancement in technology. As a result the ease with which personal information can be collected, stored and disclosed adds to the on-going challenge to protect our fundamental privacy rights. The release of the Wikileaks Bahamas files; the on-going project to implement the Bahamas Government On-Line (BGOL) initiative; and our own Data Protection Awareness Campaign are but a few reasons why we need to ensure that we take every opportunity to promote the principles of data protection (detailed in this Report) to best advantage in this information age which now prevails.

COMMISSIONER'S STATEMENT

I am pleased to present this Annual Report 2010 in the fourth year since becoming Data Protection Commissioner.

Mr. George E. Rodgers

Now is a good time to restate that our mandate is to oversee the administration and enforcement of the DPA and to enhance our mission which is "to protect and promote the privacy rights of individuals." My office is committed to assisting with the development of all information protection devices but in so doing I will continue to:-

- demonstrate leadership in promoting and protecting privacy;
- act with independence, impartiality and integrity;
- value our public officers who promote the BGOL initiative;
- be responsive to our clients; and
- work collaboratively with stakeholders as we seek to raise the awareness of data protection in our country.

I am pleased to report that the ability to capture and monitor our website statistics has been restored, albeit only within the last six (6) months of the year. During this period a total of 2608 visits were recorded and these are detailed at **Appendix 1**.

The Strategic Plan 2010-2012 that was introduced last year is beginning to yield good dividends, particularly in our effort to foster public awareness, which will be highlighted elsewhere in this Report.

Encouraging our citizens to formally register their complaints remains a challenge. Nevertheless, the number of complaints and/or queries shows signs of progress. There were six (6) complaints and thirty two (32) queries in 2010 compared to five (5) complaints and twenty two (22) queries in 2009. In 2010 I was able to visit nineteen (19) agencies/institutions interacting with three hundred and forty-eight (348) individuals in the process (prior year eighteen (18) visits and three hundred and four (304) individuals). One day visits to both Cat Island and Bimini were very well received. Other Family Island trips were planned but these were aborted due to budget constraints. I hope to visit more of the Family Islands in 2011.

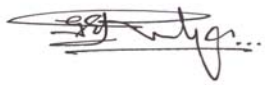
Convocation 32 of the International Conference of Data Protection and Privacy Commissioners was held in Jerusalem, Israel, during the last week of October, 2010. It was hosted by the Israeli Law Information and Technology Authority (ILITA) at the International Convention Centre, Jerusalem. It ran consecutively at the same location with a two day seminar sponsored by the Organization for Economic Cooperation and Development (OECD) I was privileged to represent The Bahamas at both events. Together, the ILITA and OECD conferences attracted over 600 participants from 50

countries comprising representatives from 39 Data Protection Authorities around the world.

The theme of the OECD event was "The Evolving Role of the Individual in Privacy Protection: 30 years after the OECD Privacy Guidelines." On the other hand, Conference 32 embarked on the theme "Privacy Generations." These conferences provided impetus for much insight into the realm of data protection and the importance of the work of the OECD. Details of the resolutions passed and reproduction of many of the discussion papers may be found at www.privacyconference2010.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, is under active consideration. The enactment of the DPA overcame the first hurdle. Secondly, The Office of the Attorney General (OAG) has been engaged to assist with producing a set of Regulations arising from the DPA. Thirdly, we continue to encourage our community to take advantage of our facilities to enhance our Case Management Skills. At this stage, the importance of the DPA in the global arena is manifested by its prominence as an element in all the Tax Information Exchange Agreements (TIEAs) that have been successfully negotiated todate between The Bahamas and some 24 countries.

I end by using this forum to thank the Acting Financial Secretary Mr. Ehurd Cunningham, and Legal Advisor, Mrs. Rowena Bethel for their invaluable contribution to the work of the ODPC. Very special thanks to my Secretary, Mrs. Sabrina Woodside and Mr. Dexter Fernander, for their untiring assistance and technical support in producing this Report.



George E. Rodgers
Data Protection Commissioner

23rd February, 2011

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 ON 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 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 securely 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

Promotion and Public Awareness

One of the functions that remain paramount in the daily activities of the ODPC is promoting general awareness of data protection in both the private and public sectors of our community. With this in mind, the Commissioner was able to forge a working relationship with a local marketing firm to launch a vigorous Awareness Campaign that began in September 2010, and will continue into the first half of 2011.

The campaign began with a redesign of the logo for the ODPC which is vividly displayed on the front and back covers of this report. Then came the production of several 60 seconds Public Service Announcements (PSAs) covering aspects of the topic "Know your data protection rights". These will be followed by topics comprising:-

- The principles of data protection;
- Defining identity theft;
- Are you ready for data protection? and
- The role and responsibilities of data controllers within the DPA.

Undoubtedly, the use of PSAs has already begun to raise the level of awareness of data protection (privacy) issues affecting individuals in their daily lives. Regrettably however, our citizens remain reluctant to formally register their complaints with the ODPC. Nevertheless, small gains are evident. As previously noted, there were six (6) formal complaints and thirty-two (32) enquiries via telephone and e-mail in 2010, compared to five (5) complaints and twenty two (22) enquiries in 2009. It was encouraging to note that the enquiries were more substantive, giving the impression that there is a greater grasp of the principles and intent of the DPA.

Of the six (6) complaints received:-

- three related to the operation of timeshare properties in The Bahamas. As these were outside the purview of the Data Protection Commissioner, they were redirected to the Bahamas Investment Authority.

- one sought our help in a matter that was more akin to Freedom of Information (FOI) than data protection. (The Commissioner advised that as FOI legislation is still pending he was unable to provide any assistance in this regard.)

- another related to a refusal to release personal information on request and, finally,

- one involved correcting personal information already held on file.

Public Education

During 2010 the Commissioner made nineteen (19) road trips/presentations to various government agencies and/or private organizations promoting the virtues of data protection directly to three hundred and forty eight (348) individuals; (prior year eighteen (18) road trips/presentations and three hundred and four (304) individuals.) Those visits included one day trips to both Cat Island and Bimini. Each visit was very well received. Resources permitting, the Commissioner intends to include more Family Islands in his schedule for 2011. (See **Appendix 2** for a Schedule of Agency visits and/or presentations).

A successful Town Meeting was held at the British Colonial Hilton on November 17th, 2010 that drew a modest crowd of 45 persons. However, the event was videotaped and will be transmitted to wider audiences via radio and television broadcasts. Guest speakers at the town meeting were:-

- Mrs. Rowena Bethel, Legal Advisor in the Ministry of Finance
- Ms. Mellany Zonicle, Director, Department of Social Services
- Ms. LaShell Adderley, Legal Counsel, Bahamas First General Insurance Limited.

The text of each presentation is reproduced at **Appendix 3**

You will note from our "Tip of the Month" feature (**Appendix 4**) that the focus throughout the year has been on educating individuals on ways to protect their privacy rights against the growing phenomenon of Identity Theft and Scam Artists. **Appendix 4** lists the various topics discussed and these may be viewed at our Website www.bahamas.gov.bs/dataprotection

Protecting the Public

The Commissioner was pleased to have been a member of the Committee that spearheaded the introduction and implementation of Electronic Monitoring in The Bahamas. Bahamians can feel a little safer in their communities knowing that the police can look forward to the use of one more tool in the fight against crime. The technology has been tested and is now in place for the Courts to order electronic monitoring as a condition of bail, which was the subject of much concern in recent months.

As a member of the Special Advisory Committee on Closed Circuit Television (CCTV) the Commissioner has submitted a set of guidance notes on the use and privacy implications of CCTV. These notes will form part of the Request for Proposal (RFP) when it is issued in early 2011.

Having been in office for the past four (4) years the Commissioner is of the view that there is a need to establish an initial set of Regulations to supplement the DPA. Consequently, in accordance with Section 30 of the DPA, which denotes that the Minister responsible for data protection may from time to time make Regulations for its orderly

functioning, the Commissioner has solicited the assistance of the Law Reform Unit of the OAG to draft Regulations covering the following subject matters:-

- Fair Processing of personal information;
- Credit References etc.;
- Sensitive Personal Data;
- Transfer of Personal information in the Public Interest; and
- International Cooperation.

Once completed, the Parliament will have to sanction these Regulations before they become law.

The Commissioner is obliged to remind both public and private sector organizations of our community that we are in year four (4) of the five (5) year grace period which allows the continued use of existing personal information (expiry date of April, 2012) without being fully compliant with Section 31(2) of the DPA. The 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."
>
> Time is running out, and all stakeholders should now be well on the way to ensuring that personal data files are updated and/or purged to promote good data protection practices.
>
> Finally, the ODPC is available to answer questions about your privacy issues and help you to protect your personal information.
>
> **Remember "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 ODPC.

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).

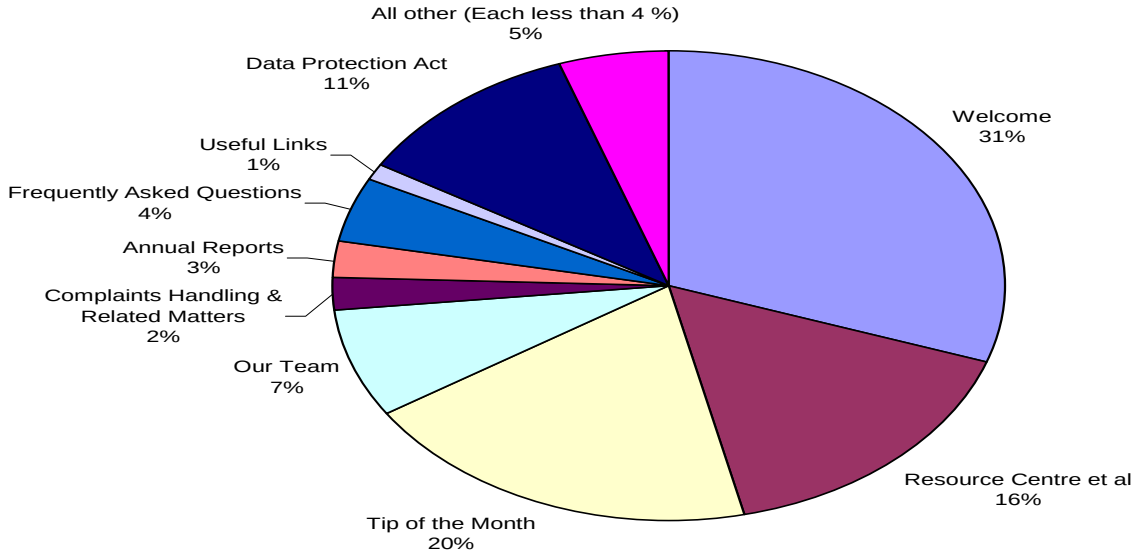
*** NB. All notices are subject to appeal to the Supreme Court under Section 24.**

Appendix 1

Website Statistics for six months
June 01, 2010 – December 31, 2010

As noted in the report last year our website statistics (on the number and subject of "hits") were inadvertently lost. A replacement software feature was not activated until mid year 2010. Consequently, the statistics below only reflect the period noted above.

Area	No. of Hits	Percentage
Welcome	790	31
Resource Centre et al	418	16
Tip of the Month	508	20
Our Team	193	07
Complaints Handling & Related Matters	064	02
Annual Reports	066	03
Frequently Asked Questions	110	04
Useful Links	033	01
Data Protection Act	289	11
All other (Each less than 4 %)	137	05
Total	2608	100



Appendix 2

Schedule of Agency Visits and/or Presentations

Date	Agency	Number of Participants
Jan. 07	Sedom Financial Services	02
Feb. 25	Bahamas Association of Compliance Officers	76
Mar. 10	Nassau Airport Development Company	04
Mar. 17	Bimini Island (consortium of Government Agencies)	12
April 20	Bahamas National Geo. Info. Services (BNGIS)	04
April 23	Int'l Finance Corporation & CARTAC	07
April 28	Cat Island (Consortium of Government Agencies	13
Aug. 24	Clifton Heritage Authority	09
Aug. 24	BTVI	15
Aug. 26	H.M. Prison	06
Nov. 17	Town Meeting (British Colonial Hilton)	45
	NON – GOVERNMENT AGENCIES	
May 31	J.P. Morgan Trust Co. (Bahamas) Ltd.	56
June 09	Commonwealth Bank Ltd.	07
June 22	Furniture Plus Ltd.	08
July 08	Bank of The Bahamas	08
July 13	Bank of Nova Scotia	10
July 27	Royal Bank of Canada	10
Nov. 04	Bahamas Insurance Association	11
Nov. 18	I.B.M. Bahamas Limited	45

Appendix 3

SPEECHES FROM THE TOWN MEETING

TOWN HALL MEETING ON DATA PROTECTION

Wednesday, 17th, November 2010

British Colonial Hilton

Presentation by Rowena G. Bethel, Legal Advisor, MOF

Introduction

The term "data protection" is just another way of describing the concept of information privacy, but more specifically, privacy and confidentiality as it relates to personal information.

For the purposes of this presentation, I will use the term "information privacy", unless I am making a direct quote, as the use of the term "data protection" is in widespread use in many instruments at the international and national levels.

I often find it helpful to lay the history and context of a subject or issue as a means of giving some idea of the "why" something is the way it is; or, simply, why it is at all. I propose to give such background history and context, in brief, on this concept of "information privacy".

Information privacy has its genesis as part of human rights. Indeed, this particular human right to privacy of personal information can be found enshrined, amongst other privacy rights, in a number of Constitutions and other fundamental freedoms and rights charters around the world.

More commonly, it is, today, found as a separate general law governing

the collection, storage and dissemination of personal information by both the private and public sectors, along the lines of our own Data Protection (Privacy of Personal Information) Act. The intention being that an individual will have a right to control the terms under which his personal information is acquired, disclosed and used.

In the early part of this decade, a survey conducted by Global Internet Liberty Campaign identified three main reasons for countries' movement towards comprehensive privacy and data protection laws:

- To remedy past injustices -many countries, notably in Central Europe, South America and South Africa, have adopted laws to remedy privacy violations that occurred under previous authoritarian regimes;

- To promote electronic commerce - These countries are said to have recognized that consumers are uneasy with their personal information being sent worldwide, and privacy laws are part of e-commerce legislation that sets up uniform rules to introduce relevant protections; and

- To ensure consistency with Pan-European laws - This is to ensure that trade with the EU will not be affected by the requirements of the EU directive, which contains a prohibition against flows of data from an EU member state to a country that does not have an adequate data protection regime in place. The EU has identified several countries as part of a "white list" that are deemed to have adequate DP regimes.

  In this respect, it should be noted that the EU, as part of its EPA negotiations with the ACP countries, sought and obtained commitments from prospective partners, to implement information privacy regulatory regimes.

International Scope

There are several international instruments that have established standards or principles with respect to information privacy. Such

instruments have been issued by the United Nations, the OECD, the Council of Europe and the European Union respectively, underscoring the importance that is accorded to these rights globally.

The recognized international principles for information privacy primarily ensure that information collected on individuals is done so lawfully, can only be used for the purpose for which it is collected, can only be disclosed in specified circumstances and that it is kept securely. The right of persons to access and amend their personal information is also a primary feature of the rules on information privacy.

The big thrust towards implementing information privacy regulation around the world took place with the explosive growth of information and communications technologies, and its pervasive use in the conduct of business and other affairs via electronic means.

The global electronic economy that has arisen from this is supported by the global information infrastructure that facilitates seamless interconnection of individual national information infrastructures (the communications networks).

Confidence in that global communications infrastructure was and remains fundamental to its effective utilization as the foundation for the global economy.

To achieve this objective i.e. the confidence in the use of the systems, countries have passed laws that are harmonized in three key areas: first of all, for the legal recognition of electronic communications and transactions conducted over the information infrastructure; secondly, to ensure the security and protection of information as well as for users of the infrastructure; and finally, to provide for the privacy of information systems and users of those systems.

The Bahamas Data Protection Act was passed in April 2003, along with the Electronic Communications and Transactions Act and the Computer Misuse Act. 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.

The ECTA and CMA came into force in June 2003 and the Data

Protection Act came into effect in 2007. [N.B. the Data Protection Act in UK was passed in 1998 and brought into force in 2003.]

Regulating Information Privacy in The Bahamas

Turning our attention now to an overview of the regime for the regulation of information privacy in The Bahamas.

Under the Data Protection (Privacy of Personal Information) Act, Chapter 324A, specific privacy principles on the collection and use of data (personal information) have been established. These are that:

(i) Data (information) should be collected and used fairly and only for lawful purposes;

(ii) Data should be accurate and kept up to date;

(iii) Data should only be kept for specified and lawful purposes, and only used and disclosed in conformity with those purposes;

(iv) Data should be adequate, relevant and not excessive in relation to the purpose for which they are kept;

(v) Data should not be kept for longer than is necessary; and lastly

(vi) Data should be subject to appropriate security measures to guard against unauthorised access, alteration, disclosure, destruction or accidental loss.

The Act also sets out a number of rights for individuals in respect of their personal data.

These are, firstly, the right of access, which mandates that within 40 days of a request an individual should be provided in intelligible form with details of any personal data being kept on him, once he has requested such.

The Act does provide some exceptions to this right, in which case, the access may be denied, such as for example, where the personal data is kept for the purpose of preventing, detecting or investigating offences, prosecutions, collection or assessment for tax, duty or similar collection, or in situations where the disclosure would be prejudicial to the security or maintenance of good order in a prison or detention facility.

An exception also exists in the case of information - (1) kept pursuant to any enactment for the protection of individuals against financial loss arising out of dishonesty or malpractice in the provision of financial services, investments and company management (i.e. investor protection measures); (2) that is subject to legal professional privilege; (3) that may be contrary to the interests of protecting the international relations of the country; (4) where the access would reveal confidential commercial information which cannot be severed from the record containing the personal information; and (5) is statistical or research data or back-up data.

The second right granted to an individual under the Act is the Right to rectification or erasure whereby, within 40 days of requesting such an individual must have inaccurate data corrected or erased.

The third right granted to an individual is the Right to prohibit the processing of personal data for the purposes of direct marketing. In this regard the Act requires that within 40 days of being requested a data controller shall erase all data kept for the purpose of direct marketing on a subject individual.

It is important to note that the Act provides data controllers with power to override the general protection afforded to individuals under the data protection principles, against disclosure of their personal information where such override is warranted in the interests of: (1) national security as determined by the Commissioner of Police or the Commodore of the Defence Force; (1) criminal investigations, prosecutions and the collection of tax, duty or similar levy; (3) protecting the international relations of the country; or (4) preventing injury damage or loss to person or property. It may also be overridden where it is a requirement of an enactment or court order; required as a part of legal proceedings or made to the data subject or on his behalf.

Application of the Act - The Act applies to the public as well as private

sectors. Its scope covers data controllers established in The Bahamas, i.e. an ordinary resident, a business entity formed under the laws of the Bahamas or someone who maintains an office, branch, agency or regular practice here, who processes data in the context of the establishment. It also applies to a data controller who is not established here but uses equipment in the Bahamas for processing the data other than for the purpose of transit through The Bahamas.

Exclusions to the provisions of the entire Act have been made in respect of personal data necessary for national security purposes, information that the law requires the data controller to make available to the public or that is kept by an individual for family or household affairs or only for recreational purposes.

Administration of the Act

Data Protection Commissioner - The Act is administered by the Data Protection Commissioner, who is a corporation sole. Mr. George Rodgers currently holds that position. The Commissioner is empowered to issue enforcement notices, information notices and prohibition notices. The Data Protection Commissioner is a high level post and is appointed by the Governor-General on the advice of the PM after consultation with the Leader of the Opposition. Parliamentarians and elected local government officials are ineligible to be Data Protection Commissioner.
"Authorised Officers" **–** the Commissioner has power to appoint authorised officers for the purpose of obtaining information necessary for the performance of his functions under the Act. These officers will have general powers of inspection, examination and entry.

Transborder data flows **–** the Commissioner has power to issue a prohibition notice where the transfer of personal information is being made to a jurisdiction that does not provide equivalent protection to data subjects. In practice, although this power exists in all other jurisdictions with data protection laws, it is seldom if ever invoked since the transfer of data to such a jurisdiction may be authorised by the data subject. Further, this prohibition is waived in those circumstances where, by contract, the recipient of the data agrees to comply with the standards that exist in the Act. The EU currently has a register of approved jurisdictions for transborder data flows by its member countries. The register currently includes Switzerland, Hong Kong and New Zealand.

Codes of Practices **–** Industry generated codes of practice are encouraged, and may be given force of law through being laid before Parliament.

Appeals Process **–** There is a right of appeal from a decision of the Commissioner to the Magistrates Court.

Prosecutions **–** The Commissioner is empowered to prosecute offences under the Act, and the time limit for prosecution of offences under the Act is one year from the date of the offence. In addition to imposing penalties, the court can order erasure, forfeiture or destruction of the data concerned.

Departments of Social Services and Rehabilitative Welfare Services Responsibilities under The Data Protection (Privacy of Personal Information) Act, 2003

Wednesday 17th, November, 2010

Presentation by Mellany Zonicle, Director of Social Services

In the Departments of Social Services and Rehabilitative Welfare Services social workers/probation officers play major roles in meeting the needs of a cross-section of Bahamians who are at risk temporarily, suffer from permanent disabilities or just interested in adopting a child.

The assistance or advice given is considerably dependent upon the professional relationships developed through the sharing of information. In essence social workers/probation officers cannot properly and effectively serve their clients without asking for information on aspects of their personal lives and later contacting their relatives, friends or employers to ensure the information is correct.

Further, given the unique nature of the service to be provided it must be determined what information is to be held as confidential, what aspects of the information should be shared, and with whom the information needs to be shared.

A brief identification of the Departments' various divisions underscores the volume and diversity of personal information required.

1. Children and Family Services

    a. child abuse matters
    b. adoption and foster care
    c. residential placements for children
    d. custody matters
    e. domestic violence matters

2. Community Support Division services for the following are subjected to a means test.

    a. food assistance
    b. financial assistance

3. School Welfare Division

a. National Lunch Programme
b. Working with at risk students

4. Health Social Services at Sandilands Rehabilitation Centre and Princess Margaret Hospital

    a. Determining eligibility for med cards and financial medical assistance
    b. Case management of at risk out and in patients at SRC and PMH

5. Senior Citizens

    a. Working with seniors at risk
    b. Day care and residential placements

6. Disability Affairs services are also subjected to a means test

7. Rehabilitative Welfare Services

    a. Community supervisions of person before the courts
    b. Operation of the Simpson Penn and Willie Mae Pratt Centers
    c. Welfare services at Her Majesty's Prison

Most of the two Departments' responsibilities can be found in many pieces of legislation, the major ones being the Penal Code, the Adoption of Children's Act and the 2007 Child Protection Act. Since the enactment of the 2003 Data Protection (Privacy of Personal) Information Act the Department's work has been impacted. However, adhering to the provisions of the Act has not been a challenge. Before and after this Act social worker/probation officer had an obligation to respect client's rights by keeping in confidence information obtained from or about them?

Information gathered forms the record of work that has been done with clients on a one time basis or over a period of time. Important decisions about an individual or individuals are made on the basis of the information taken. If the information is incomplete, inaccurate or unfair client's rights may be at risk or they could be denied a better benefit or service they would need.

The information gathered and recorded also helps social workers/probation officers monitor their work and ensures someone else can continue the work when necessary. This information may be on paper or electronic. Departments' records are stored in a secure place and protected from unauthorized use.

It can not be over-emphasized that good record keeping is an important part of the social worker/probation officer task. Records should have clear, straight forward language, be concise and accurate. They should clearly differentiate facts, opinion, judgments and hypothesis.

If the one does not agree with aspects of the information on one's file one can ask for a file to be changed, or if that isn't possible, one's views can be recorded on the file.

For example well-kept records are essential to good child protection practice and the presentation of court reports. Safeguarding children requires information to be brought together from a number of sources, and careful professional judgment to be made on the basis of that information at any stage. Judgments made, actions and decisions taken should be carefully recorded. Where decisions have been taken jointly across agencies or endorsed by a Supervisor this should be made clear on the file.

As previously mentioned, both Departments must safeguard the confidentiality of the personal information which it holds about individual who require its services. However when the issue of the disclosure of confidential information to another person or body arises, the Department must always ensure that such disclosure is lawful. The Departments will always record their reasons for deciding not to observe any duty of confidentiality it owes to a person who is the subject of the information that must be disclosed.

The Departments of Social Service and Rehabilitative Welfare Services are well aware that under the Data Protection (Privacy of Personal) Information Act, 2003 the subject of a record has the right to see their information.

a. if they are the person whom the file is about
b. if they are legally responsible for someone who is not capable of asking to see the file for themselves

Despite what I just said, there may be some information in a person's file which he/she does not have the right to see because it may include information about other people whose rights have to be protected. Further, the denial of information is possible under the following circumstances:

a. the information has to be withheld by law
b. where disclosure could cause serious harm to the physical or mental health or medical condition of some one
c. disclosing the information could stop the police preventing a crime or prosecuting.

In May of 2009, all senior staff of the Departments Social Service and Rehabilitative Welfare Services met with Data Commissioner Rodgers and are now actively changing the culture of these Departments in the way they store and record information. Officers have adhering to the following principles:

1. Obtaining information first hand from individuals concerned and building good and honest communication

2. Only collecting personal information that is really needed and retaining it for as long as absolutely needed.

3. Informing the individual about the need to record information and why it is necessary to collect that personal information

4. Using lawful, fair and reasonable methods to collect information that is not readily available

5. Checking for accuracy before using personal information making sure it is current, relevant, complete, accurate and not misleading

6. Using personal information only for its intended purpose(s)

7. Limiting and / securitizing third party disclosure of personal information.

Protecting the rights of persons who must use the services of the Departments of Social Services and Rehabilitative Welfare Services is of paramount concern; therefore the provisions of the 2003 Data Protection (Privacy of Personal) Information contribute to the accountability and efficiency of the two Departments.

DATA PROTECTION ACT TOWN MEETING
BRITISH COLONIAL HILTON
NOVEMBER 17th, 2010 at 7:00 pm

"Data Protection in the Insurance Industry"

Presentation by Mrs. La'Shell Adderley

Undoubtedly, under the Data Protection Act, 2003 there are benefits and obligations for both the insured and insurance companies. The primary objective of this paper is to strike a somewhat difficult balance between an individual's right to access personal data collected on the one hand, and an insurance company's legitimate interest and obligation to abide by stringent data protection mandates on the other.

The difficulty of balancing the rights of both parties becomes even more apparent when the insurance company, pursuant to statutory exceptions, denies a client access to their private information or data.

In order to ascertain the legal rights of the insured, and the insurance industry, this paper will focus on four (4) key areas: firstly, a brief introduction to the domestic insurance industry; secondly, obtaining & protecting private information of the insured; thirdly, various rights of the insured in relation to their personal data; and lastly, the insurance company's right to deny access under exceptions to the general rule.

Domestic Insurance Industry

The domestic insurance industry is mainly divided into two classes of insurance business: long term and general. Long term refers to life and health products, whereas, general refers to property and casualty i.e houses, vehicles, boats etc.

Insurance companies utilize the services of insurance intermediaries to sell and service their products. The new domestic Insurance Act, 2005 defines an insurance intermediary as a broker, agent, sub-agent, adjuster, risk manager, consultant, or such other persons who give advice by way of directly offering, advertising or on a person-to-person basis in respect of an insurance product and includes the promotion of such product or the facilitation of an agreement or contract between an insurer and a customer.

With the enactment of the Data Protection Act, 2003 a living individual now has a statutory right to privacy with respect to their personal information which cannot be divulged to a third party in the absence of their consent. Additionally, the

individual has a right to access their personal files. The Data Protection Act also regulates the activities of organizations that use information relating to individuals and makes it essential for organizations to manage personal data effectively and efficiently.
The question is asked: Why should insurance companies be so concern about the Data Protection Act? Perhaps we can get the answer from Zurich UK who was fined over $3.6 million dollars over the loss of 46,000 customer's personal information and breach of the Data Protection Act.

Obtaining Information

Locally, information is obtained from a client or data subject at 3 critical stages.
Firstly, there is application or proposal stage. During this stage the individual will divulge vital personal information on their health, driving and claims history and property value etc.
The application or proposal form should include a consent provision which will allow an insurance company to release personal information to their subsidiary companies, agents, brokers, sub-agents, salespersons, reinsurers, legal advisors, loss adjusters, surveyors, private investigators, medical practitioner, mortgagee or loss payee.
In the very near future, the Central Bank of the Bahamas will establish the nation's first privately -owned credit bureau. It is also foreseeable that the insurance industry will seek regulatory approval to establish a database containing claims information.
In order to forward clients' information to the Credit Bureau or an insurance claims database, it is incumbent upon the insurance company and/or intermediaries to not only obtain the client's consent but also ensure that the client is aware of the purpose and type of information that will be reported to such entities.
In the second stage the policy is in force. Premiums are paid and continuous updates are made by the client during the length of the policy.
Thirdly, there is the claims stage where additional information is ascertained to determine whether a claim is payable under the policy, and, if so, the correct amount of the payment. To assist in ascertaining whether a claim is payable under a policy, an insurance company may outsource work to a loss adjuster, private investigator, medical practitioner, surveyor, or attorney.
If the claim involves a 3rd party or witness, consent is required because personal information is shared in the claims stage.
In order to effectively and efficiently achieve the primary objectives of the Data Protection Act, the Data Controller must satisfy the following key principles of the Act in relation to the collection, quality and use of personal data. Accordingly, the rules of Data Protection mandate the following rights of an individual:

a) Fair and lawful collection of Data: This means that the necessary consents are obtained in order to pass the information onto third parties.

With respect to Private Investigators, insurers should ensure use of a licensed private investigator and contractually engage them on the basis that the company will abide by Data Protection Act legislation. The Insurance Company should also obtain appropriate indemnities from a private investigator in relation to any non-compliance with Data Protection Act.

Of notable importance, an insurance company can "outsource responsibility but not accountability".

b) The data should be accurate and kept up to date: Incorrect data must be corrected. Companies should also have appropriate procedures in place to check the accuracy of data

c) The data shall not be used or disclosed in any manner incompatible with the purpose:

For example, Insurance companies must ensure that personal data is NOT disclosed to a tele-marketing firm or that former employees do not have access to personal data.

d) The data shall be kept accurate, relevant and not excessive

e) 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): Insurer's should have a written retention policy with respect to how long the policy holder's information will be kept. The Statute of Limitation's Act will provide a useful guideline to both long term and general insurers in relation to the retention of information.

f) Appropriate security measures shall be taken against unauthorized access to, or alternation, disclosure or destruction of, the data against their accidental loss.

The appropriate security measures include technical as well as organizational measures. Adequate technical measures include, but are not limited to, firewalls and encryption. Particular focus should be placed on the security of personal data held on portable devices such as laptops and memory sticks.
The appropriate organizational measures include, but are not limited to, robust staff training and strict IT, Human Resources and Compliance policies.

The recent case of a British Insurance company highlights the importance of encrypting data on any device to ensure that information is safe even if it gets in the wrong hands.

According to the July 8th, 2009 issue of Computer Weekly, Jubilee Managing Agency which is part of Lloyds, lost an unencrypted disc which contained the personal details of 2,100 people and was subsequently found in breach of the Britain's Data Protection Act by the Information Commissioner's Office.

A review of the Insurance Company found a lack of detailed data security procedures and policies, and insufficient staff training in the agency. Even more alarming was the fact that some of the data on the lost disk referred to policies, in some cases over 10 years old, that had expired or been cancelled, as well as information on policyholders who had since died or change address.

The HEAD of enforcement and investigations at the Information Commissioner's Office (ICO) stated:

"This case is not only a reminder that the appropriate safeguards should be in place to protect personal information, but that organisations must ensure information is accurate and up to date. Organisations should only retain personal information for as long as necessary. It is a matter of some concern to us that expired policies, including financial details, were still available and stored on unencrypted devices.

We urge all CEOs and their senior management teams to ensure data protection is treated as a corporate governance issue affecting the whole organisation. All organisations need to make sure that safeguarding the personal information of customers and staff is embedded in their organisational culture."

In another case that occurred earlier this year, London Mutual Insurance Society, an insurance company, was found in breach of the Data Protection Act after laptops containing 2,000 customers' details went missing from its offices. The company was criticized by the ICO for failing to take adequate precautions to safeguard customer data after eight laptops in total went missing from the company's Edinburgh offices – two of which held customer data.

Insured's Right to Access

The Data Protection Act mandates that at any point the insured has a right to request and obtain (within forty days) any and all information held by their insurance company or intermediary.

Once a client receives their personal information and he doesn't agree with the information on file, the client has a right to have the inaccurate information rectified or erased.

Although the Data Protection Act gives the insured the right to access their personal information, there are exceptions to the general rule whereby the insured is denied access to their personal data.

Exceptions to the General Rule

In particular, Section 9 provides ten exceptions whereby an individual's right to access personal information could be denied. Needless to say, an insurance company or intermediary can refuse to release any document to which one of the Section 9 exceptions apply.

The insurance industry would likely utilize the following important exceptions found under Section 9 of the Act:

a. The personal data is one whereby a claim of privilege could be maintained in proceedings in a court in relation to communication between client and his attorney; or,

b. The information would reveal confidential commercial information which cannot be severed from the record containing the personal information for which access is requested

With respect to privilege, the United Kingdom Court of Appeal case of ***Three Rivers District Council v Governor and Company of the Bank of England*** [2003] QB 1556 defines lawyer client privilege as "*communications between lawyers and their clients whereby legal advice is sought or given. Legal advice includes advice as to what should prudently and sensibly be done in the relevant legal context".*

Of notable importance, Section 13 of the Data Protection Act overrides any restrictions on or exceptions to the disclosure of personal data. For example, exceptions to the disclosure of personal data include:

i. safeguarding national security;
ii. Protecting international relations;
iii. Requirement by law or order of a court; or
iv. Required for the purpose of obtaining legal advice or for the purposes of, or in the course of, legal proceedings in which the person making the disclosure is a party or a witness.

Now you are probably asking yourself the question what does all of this mean in layman's terms? Let's use the illustration of Mr. John Doe who takes out a homeowners insurance through an Agent of ABC Insurance Company. Shortly thereafter, Mr. Doe experiences a home invasion and valuables amounting to $50,000 dollars are stolen from his home. ABC is suspicious and suspect that they are dealing with a fraudulent claim. Subsequently, Mr. Doe commences legal action against ABC because they are taking far too long to settle his claim. ABC then retains both a Private Investigator and an Adjuster to investigate the claim. In turn, ABC sends both reports to their Attorney for legal advice.
Meanwhile, Mr. Doe decides to exercise his rights under the Data Protection Act and request a copy of his personal information held on file at ABC.
At this point, ABC can give Mr. Doe access to his personal data except for any document which falls into the exceptions. Clearly, ABC will use **the** exception found in Section 9 (g) and (i) namely:

a. A Claim for legal privilege over the Loss Adjuster and Private Investigator reports. However, I hasten to add that a claim for privilege must be justified.

b. The information would reveal confidential commercial information which cannot be severed from the record containing the personal information for which access is requested

What if Mr. Doe is being investigated by the local police and the FBI with respect to an international stealing ring? All documents held by ABC must be released to the Police.
What happens if an individual's data is released to a 3rd party without his consent? If an insured becomes aware that their personal data has been divulged to a third party without their authority the individual can report this breach to the Data Protection Commissioner for further investigation.
One of the stringent provisions of the Act is that where an offence is committed by a body corporate and it is proved to have been committed with the consent, connivance or neglect on the part of a director, manager, secretary or other officer of that body corporate, **that person** and the body corporate shall be guilty of an offence.
Therefore, if the Claims Manager of XYZ insurance company discuses Jim Jones latest medical report with his arch rival, not only would XYZ Insurance Company be guilty of an offence but the Claims Manager would have committed an offence under the Act in his personal capacity.
In closing, I urge insurance companies to fix their roofs whilst the sun is shining.

Appendix 4

TIP OF THE MONTH

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

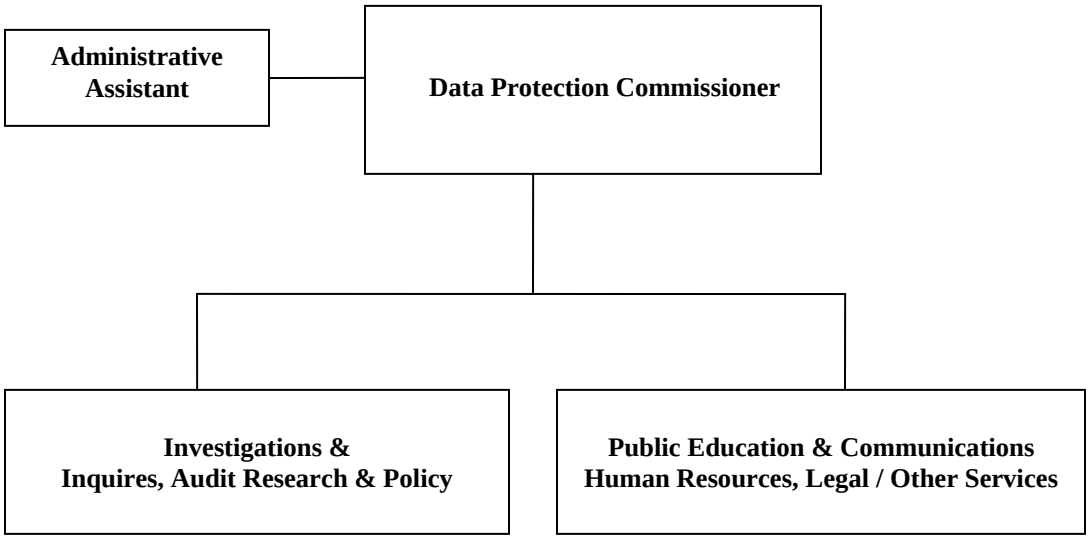
January	Why worry about my Privacy!
February	We're here to help you protect your Privacy.
March	Be generous but protect your Privacy.
April	Learning about Identity Theft.
May	"Botnets" What are they?.
June	ID Scanning in public places.
July	Learning about Identity Theft. -2 (It's Vacation time again).
August	Privacy in our schools.
September	Terms you should know to protect your privacy.
October	Learning about Identity Theft -3.
November	Offences under the Computer Misuse Act, 2003.
December	Identity Thieves want your Personal Information.

The focus has been on protecting the privacy rights of individuals against the growing phenomenon of Identity Theft and the proliferation of scam artists.

Appendix 5

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

- Investigate complaints received from individuals under Section 15 of the DPA.
- Establish whether individuals have had their privacy rights violated.
- Determine whether individuals have been afforded their rights to access to their personal information.
- Seek to provide redress and to ensure violations do not recur where privacy rights have been violated.
- Mediate and conciliate, with a view to taking corrective action, if necessary; 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

- Assess how well organizations comply with the provisions and spirit of the DPA.
- Conduct compliance reviews of the function and/or work of a Data Controller or Data Processors, with regard to the application of the Act outlined in Section 4 of the DPA.
- Receive, analyze and provide comments and recommendations on Data Protection issues affecting The Bahamas.
- 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 programme 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.
- Plan and implement a number of public education and communication 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.

Appendix 6

FINANCIAL STATEMENTS

Receipts and Payments for the period January 1st 2010 to December 31st 2010

(Expressed in Bahamian Dollars)

Receipts

	2010	2009
Contribution provided via the Ministry of Finance (Note 1)	131,723	140,229
Total Receipts	**131,723**	**$140,229**
Payments		
Salary & Allowances (Note 2)	100,900	$133,900
Awareness Campaign	22,313	-
Travel & Subsistence	836	340
Training & Related costs	4,684	4,244
Office & Computer Equipment	714	200
Furniture & Fittings (Note 3)	-	-
Miscellaneous Expenditure	2276	1,545
Total Payments	**$131,723**	**$ 140,229**

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. 2009 figure includes gratuity in respect of the prior contract.

   (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

Second Floor
Cecil Wallace-Whitfield Centre,
Cable Beach
P. O. Box N-3017
Nassau, Bahamas
Tel: (242) 702-1552/ 702-1534
E-mail: dataprotection@bahamas.gov.bs
www.bahamas.gov.bs/dataprotection