Explanatory Memorandum
Data Protection Policy and Bill

A. Background

1. Introduction
The Ministry of Public Administration and Information (MPAI), through extensive consultation with the public sector, the private sector and academia, developed ***fastforward***, the National Information and Communications Technology (ICT) Strategy for Trinidad and Tobago. Electronic commerce ("e-commerce") has been identified as an important strategic driver for economic growth, particularly in developing countries. In order to take full advantage of the opportunities for business and consumers that is offered by e-commerce, we must have a clear and predictable legal environment that can be trusted by citizens, institutions and businesses. Two key areas in which legislation is required are Data Protection and Electronic Transactions. The Data Protection Policy forms the basis of the Data Protection Bill, which will be the first stage of the legislative renewal required to fully achieve the objectives of ***fastforward***.

2. Legislative Approach
The approach taken in the Data Protection Policy and Bill is flexible, taking into account both the need to have principles in place to assure the citizens of Trinidad and Tobago and people who do business with Trinidad and Tobago that rights to personal privacy are respected and the need to ensure that the regulatory regime does not overwhelm the public and private sectors with new responsibilities that are unrealistic and burdensome.

A. Privacy Protection by Public Authorities
Following a model that uses the Government of Trinidad and Tobago as the leader in the protection of personal privacy, the Policy and the Bill make privacy protection by public authorities mandatory. The protection of personal privacy has always had a high value in Trinidad and Tobago—indeed it is value enshrined in the Constitution—and it has been implicitly recognised in the *Freedom of Information Act, 1999*. While citizens have a right to information about their Government, this right must be balanced with the rights of individuals to maintain and respect personal privacy. The Data Protection Policy and Bill clarify and extend these rights and give additional guidance on how competing interests may be balanced. Thus, Government is subject to specific responsibilities regarding data sharing and data matching that recognise the importance of Government as a holder of information about individuals.

B. Independent Data Commissioner
The Policy and Bill provides for an independent Data Commissioner to deal with complaints and appeals from decisions made by heads of public authorities

about personal information and requests by individuals for access to their own information or correction of that information. The Data Commissioner provides a credible source of expertise, authoritative decision-making, and disinterested resolution of disputes. It is intended that the decisions and guidance of the Data Commissioner dealing with data protection by Government will provide the leadership that will be needed to integrate the values of privacy protection into the business values of the private sector in Trinidad and Tobago.

With respect to the private sector, the Policy and Bill emphasize the importance of the Privacy Protection Principles. These Principles represent good business practice and should be promoted as part of the general business ethic of the country and part of what aware consumers should expect of businesses to which they entrust their personal information. The Policy and Bill therefore stress education and promotion as important elements of successfully integrating the Privacy Protection Principles into the daily life of citizens.

The Data Protection Commissioner will have a role in promoting these values, as will other stakeholders, such as industry organisations, industry regulators, consumer protection agencies and Government as a whole. To promote more focused acceptance and adherence to the Principles, it is expected that industry groups or even individual larger corporations will develop codes of conduct that will translate the higher level Privacy Protection Principles into more detailed compliance policies that will reflect the needs of particular industries, the type of information they collect and the needs of their customers. The co-regulation approach that is being espoused in the Policy on Electronic Transactions is also being promoted in the Policy on Data Protection.

C. Co-Regulation and Codes of Conduct

For example, a bank will have different concerns about what constitutes consent of a customer to use information than will a newspaper dealing with subscribers. Medical practitioners and their patients have different needs and concerns than telephone subscribers. Codes of conduct allow groups to particularize the Privacy Protection Principles and establish mechanisms for dispute resolution, among other matters. To maintain a consistent application and interpretation of the requirements of the Privacy Protection Principles, the Policy and Bill provide a mechanism for the Commissioner to approve codes of conduct, taking into account certain criteria, including avoidance of anti-competitive conduct. The comparative expertise of both groups are being drawn on: banks, for example, are most familiar with the types of information they collect, the opportunities to introduce inaccuracies into the system, where the opportunities lie to use information for a purpose for which it was not collected and so on. They are also in a good position to set up the systems, approvals, safeguards, reporting lines of responsibilities, training sessions and other activities that will be needed to implement a programme of data protection. In these areas, they have greater expertise than a Data Commissioner. The Data Commissioner, on the other hand, has a broader view of the issues, is more aware of international practices,

of problems that have arisen in other jurisdictions, and can take are more disinterested and longer term view of such matters as the potential for anti-competitive conduct or taking an overly narrow point of view on a matter. The co-regulatory structure intends to rely on both sets of strengths.

D. Some Codes of Conduct May be Mandatory

The general approach of the Policy and Bill is promotion of the General Privacy Protection Principles and voluntary development of codes of conduct among private sector groups, organisations, or industries. In some cases, however, the protection of personal privacy and personal information will be so important that voluntary development of codes of conduct or voluntary compliance will not be sufficient to either protect individuals or create the environment of trust and confidence that is needed for Trinidad and Tobago to interact globally. In these cases, the Policy and Bill create a structure that will allow the Data Commissioner to require the development of codes of conduct and impose a time limit on development to avoid delay. Some of the areas that might be subject to mandatory codes of conduct include the health sector, the financial services sector, credit agencies, and regulated professions (e.g., accounting and health care professions).

E. One Example of a Mandatory Code would Deal with Health Authorities and Health Information

Although a number of health authorities might generally be considered to be public authorities and subject to the provisions of the Policy and Bill relating to Government, the protection of personal information in the health sector has a number of special issues attached to it. The general Principles of Privacy Protection apply, but matters relating to consent, for example, require particular care depending on the situation. For this reason, the Policy and Bill are structured to allow issues relating to protection of personal privacy in medical records and the health care system generally to be dealt with on a more specific and targeted basis.

In selected cases—most likely those where the development of a code of conduct has been mandated—the Minister may make the application of a code mandatory by an order that is placed before the House and subject to a negative resolution of the House. The Data Commissioner would play a role similar to that which he would play for the Government with respect to the mandatory private sector codes by hearing appeals and reviewing decisions and data protection practices.

F. Summary of Approach

In sum, the legislative approach taken in the Policy and Bill is a combination of the voluntary and mandatory with Government taking a leadership role in ensuring that the citizen's right to privacy is protected and promoted. This Policy and Bill take a ***sectoral approach*** to data protection, which is appropriate for developing countries such as Trinidad and Tobago as it allows for innovation in

various sectors and is not as restrictive and costly as the comprehensive approach. This approach is adopted by countries in North America and the Caribbean which are some of Trinidad and Tobago's major trading partners.

The Trinidad and Tobago Policy and Bill on Data Protection draws on a number of sources, including the OECD Guidelines, the EU Directive, the Canadian Standards Association Standard on Protection of Personal Privacy, and legislation in a number of jurisdictions, including Canada, Canadian provinces, New Zealand, Australia, the United Kingdom, and Ireland.

B. Part I: General Principles of Protection of Personal Privacy

The General Principles of Protection of Personal Privacy that are used in this draft Policy and Bill are drawn from the Schedule of the Canadian Federal legislation, which are the principles set out in the National Standard for Canada entitled "Model Code for the Protection of Personal Information," CAN.SCA-Q830-96. The Model Code was developed through a consensus process undertaken by a technical committee overseen by the standards development organisation, the Canadian Standards Association (now "CSA International"). The committee was struck according to a pre-established matrix of participants representing different interests, including consumers, technical advisors, telcoms, banks, and governments.

The decision to use a multi-party standards development approach was partly in reaction to the initiative of the European Community, which had tabled a tough data protection directive that demanded that member states put in place legislation to meet a new higher standard of protection and provided that they must not transfer data to jurisdictions where there was inadequate data protection—however that might be defined.

The approach taken by the Canadian standards development technical committee was inspired by quality management standards that were development and implemented around the world, such as ISO 9000 or ISO 14,000 dealing with environmental management systems. The Committee took the OECD Guidelines as its starting point and through a sub-committee process began to adjust the OECD guidelines to requirements that would fit the modern commercial state. When the draft standard was published for comment, most businesses believed it was a sound basis for self-regulation, while others, including the Privacy Commissioners in the provinces and the Federal Privacy Commissioner, believed it would be more effective as a basis for legislation.

When the Canadian federal government decided that legislation was appropriate, the CSA Code remained at the heart of the legislation and sets out the obligations that must be met by any organisation subject to the Act. The intention

is that the General Principles set out in Part I of this Policy and Bill will operate in a similar fashion. Each Principle is accompanied by its own commentary, elaborating on the basic structure of the Principle.

Principle 1: Accountability
Accountability is the cornerstone; each and every organisation that abides by the code, whether on a voluntary or mandatory basis, is responsible for the information under its care and control. Accountability is highlighted by the need to name and designate an officer—preferably a fairly senior officer—who is responsible for data protection within an organisation.

Principle 2: Identifying Purposes
This standard requires that the purposes for data collection be identified. Technically, the standard is silent on whether the purposes are legitimate, fair, lawful or acceptable to the individuals whose information is involved. In is only in conjunction with the consent clause, Principle 3, that these issues come into play. The intent, however, is that the provisions requiring identification of purpose should be sufficiently rigorous, precise and non-theoretical that genuine consent is possible.

Principle 3: Consent
This provision regarding consent is actually stronger than the original OECD principle, which simply states that data should not be disclosed or used for purposes other than those originally specified without consent. The Canadian CSA consent principle, on the other hand, insists on the knowledge of the data subject and consent for collection, use and disclosure. The concept of consent raises a number of issues, however, including whether the consent is informed, whether the individual is capable of giving consent (one reason why medical records are being treated as a separate issue under the Policy and Bill), and whether there are conflicts of interest between those who allegedly give consent and those who use the data. In practice, many of these issues will have to be dealt with on a case-by-case basis and in developing codes of conduct that relate to more particular situations, industry needs, and so on.

Consent may be implied, but one might argue that it should be explicit where more sensitive forms of data—for example, data about health—are being collected or used.

Principle 4: Limiting Collection
There is an obligation to show that the information is necessary for the purposes for which it is to be collected, which must be specified. One should look to the reasonable person test to determine what might be necessary for the purposes—would a reasonable person, in possession of the relevant facts, regard the collection as necessary for the purpose?

Principle 5: Limiting Use, Disclosure and Retention
This distinguishes among use, disclosure and retention. Use refers to the processing and treatment of data within an organisation and may or may not involve disclosing the information. Disclosure focuses on release of the information to a third party; depending on the circumstances, disclosure may occur to a subsidiary or division of a particular corporation. It is likely that the disclosure need not be to a separate legal person to constitute disclosure, but rather one might examine such issues as the purpose for which consent was given and collection was made. This is an example of how these principles can inter-relate. Organisations should have policies in place regarding retention and, eventually, destruction of data—this relates to issues of security and safeguards noted in Principle 7.

Principle 6: Accuracy
This Principle is key to the entire policy. However, gathering new data may not be necessary if the purpose for which the data was originally gathered is no longer relevant: it was important that it be accurate originally, but may no longer be important. In that case, it may be intrusive to regularly update the data. On the other hand, if decisions are going to be made based on older data, then updating would be appropriate. The focus here is on the interests of the individual rather than the organisation.

Principle 7: Safeguards
Privacy is meaningless unless there are safeguards to protect the information. As the Principle notes, there is a balance between sensitivity of information and the cost and sophistication of the security mechanisms needed to guard it. Safeguards refers to physical security—doors, locks, gates, walls—and computer security—firewalls, encryption, access codes—as well as such matters as doing security checks on personnel, sub-contractors, repair people and others who may have access to data. In many situations, on-going training and compliance programmes will be needed to meet security requirements.

Principle 8: Openness
While the General Principles stress the need to limit and control the collection, use and disclosure of personal information, the systems dealing with privacy protection should be open. Accountability demands that people, particularly individuals who believe that their information is being held or collected by an organisation, be able to learn about the collection, retention and disclosure practices of the organisation. While the information is not transparent, the system should be. Many organisations that routinely collect data publish a Privacy Policy. Whether or not the organisation adheres to a specific industry code of conduct, the policy sets out what its internal policies are: for example, who is responsible for the privacy policy within the firm; how individuals may correct or access their data; how individuals may challenge compliance with the policy and so on. Establishing a policy and a system for privacy protection is a good business

practice and may, in certain cases, be required by either a Data Commissioner or a sectoral regulator, such as a telecommunications regulatory authority.

Principle 9: Individual Access
This requires that the organisation not only inform the individual about what data it holds, but also what use it makes of it. There is also the right to find out to whom the data may have been disclosed. This is broader than many access rights granted to individuals pursuant to public sector access legislation.

Principle 10: Challenging Compliance
The authors of the CSA Code considered this provision to provide the broadest basis for complaint in any data protection code. An individual has the right to challenge an organisation's compliance with any of the provisions of the Code, whether or not the alleged non-compliance directly affects the individual. That is, the individual does not have to be the subject of the data in question. This is related to the provisions to be found in Part II related to whistle-blowing. Persons other than the individuals whose data is being collected may be aware of violations of compliance, particularly about matters such as security or disposal practices. It is important that they be able to bring non-compliance to the attention of the appropriate authority, who may in the first instance be the designated official in the organisation who is responsible for data protection. If that is ineffectual, then the possibility of a complaint to the Data Commissioner exists.

C. Other Principles Governing the Data Protection Policy and Data Protection Bill

Part 1: General

1.1 Definitions:

"contact information" relates to information that is required to deal with someone at a place of business. There is no intention to make it difficult to reach either a public official or an individual at his or her place of business who deals with the public. Thus, it would be possible, for example, to compile a company directory or put a directory of government employees on the Internet on an e-government site without violating the provisions of the Policy and Bill.

"data matching" can yield vast new forms of information beyond what the original information was intended to convey and is consequently subject to oversight and control of the Data Commissioner.

"head of a public authority" is generally intended to be the individual who is the most senior person or the head of the organisation; it is not necessarily the same individual who will be responsible for data protection issues on a daily basis according to the Data Protection principles. In many cases, the titular head of the public authority will delegate some responsibilities regarding data protection to the person who is identifiably responsible for data protection issues on a daily basis.

"Health care body" is intended to cover all institutions giving some form of health care. The intention of the Policy and Bill is to treat health information and health records, whether held by a "health care body" or a health worker such as a doctor or other health care practitioner separately through the development of mandatory codes of conduct dealing with either activities, types of information or organisations. Since protection of personal privacy in the health care field can be complex and requires careful co-ordination among the stakeholders, health care bodies are separated from other public authorities to whom the Policy and Bill apply in a more general fashion.

"Personal information" as defined in the Canadian federal *Privacy Act* includes information relating to race, national or ethnic origin, colour, religion, age, marital status or the individual. It may also include such matters as the information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved. It includes the address, fingerprints, or blood type of the individual.

The Canadian federal Act also includes as "personal information" the personal opinions or views of the individual where they are about another individual or

about a proposal for a grant, an award or a prize to be made to another individual by a government institution. It also includes correspondence sent to a government institution by the individual that is implicitly or explicitly of a confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence.

The name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual can also be considered personal information.
This level of detail may be more appropriate in guidance documents that should be prepared to educate the users of the Policy or Bill.

“Privacy impact assessment” is a means of ensuring that privacy issues remain in the forefront of government decision-making and that barriers to the protection of privacy are not inadvertently introduced through new legislation or programmes. The Data Commissioner would be expected to produce guidelines on the conduct of privacy impact assessments. Assessments, however, would examine such matters as whether programmes or legislation could achieve objectives without additional collection of personal information, what the minimal collection would be, how consent could be obtained, what particular security measures might be required, and so on. In addition to ensuring that any invasions of personal privacy were minimal, they would require a plan of collection, retention and disposal of data.

“Public authority” draws on the definition used in the *Freedom of Information Act, 1999*, with the exception of deleting a regional health authority established under the Regional Health Authorities Act, 1994. The regional health authority is found under the definition of “health care body,” above.

“Record” is a broad definition and matches that found in the Policy and Bill on Electronic Transactions.

Part II: Principles Relating to the Office and Powers of the Data Commissioner

The provisions relating to the appointment and terms and conditions of appointment are drawn from legislation in several jurisdictions, including Canada, Canadian provinces, the UK, Ireland, New Zealand and Australia. In many cases, an Access to Information or Data Commissioner or Privacy Commissioner (the functions may be dealt with together in one individual or one office or separated) is an officer of Parliament to emphasise independence from the day-to-day operations of government. While in no case in the appointment life-long, there are elements of judicial appointments attached to the appointment of a Data Commissioner. Usually there is some means of ensuring that the salary of the Commissioner is determined and paid independently like that of a senior judge so that remuneration cannot be thought to be a means of influencing the independence of the Commissioner.

The term of appointment of a Commissioner is relatively long: five, seven or even nine years. In some cases, he or she may be re-appointed, but during the term of office, removal may only occur for cause (including mental and physical disability). In some cases removal may only occur though a vote of both houses of Parliament. In all cases, a Commissioner has the choice of resigning for whatever reason he or she considers appropriate.

It is an important position and the individual appointed should be treated with the deference appropriate to the power of the position and the integrity and credibility that the appointee is expected to bring to the position. It should not be thought of as a partisan position, which is reflected in both the need for multi-party consultation before appointment and the fact that the Commissioner reports to Parliament as a whole during his or her term of office.

The Commissioner should follow the general precepts and rules of the public service commission in hiring staff, but should not be constrained in hiring specialists and experts on an occasional basis to meet particular needs—keeping in mind at all times that public funds are being spent and must be spent appropriately.

The Commissioner has two broad types of functions. One function involves promoting the privacy principles in the very broadest sense: speeches, brochures, TV spots, advertising, workshops, and establishing guidelines to improve compliance—all these are legitimate activities to promote the values of protection of personal privacy. These functions are generally found under the section relating to “duties.”

The second function is making binding determinations regarding compliance with the General Principles. The Commissioner would only have such a binding role with respect to public authorities and those organizations that were subject to mandatory codes. The Commissioner also has a role in approving codes of

conduct developed by industry organisations and others. The general powers of the Commissioner relate more to these functions. A distrinction is made between the powers of investigation by the Commissioner of a matter within the purview of a public authority and those within the private sector. A search warrant is not required for entry into public buildings and questioning of a public authority, although advance notification is given. There are no provisions for the external authorization of a search warrant, since it is assumed that a public authority will be operating in the public interest, as is the Commissioner, and that their ultimate interests are not opposed. Consent is thus considered to be implied in this matter. As discussed below, there are special provisions regarding entry and investigations involving privacy protection of the courts and Parliament.

In contrast, where an investigation is being made of the privacy protection practices of a private sector body and where an order might be given regarding compliance with a mandatory code of conduct, a warrant is required for entry or removal of papers.

There are protections surrounding investigations conducted by the Commissioner. Consistent with the objectives of the office, the Commissioner and his or her staff are expected to maintain all information that comes their way in the course of their duties in confidence. Such information may be disclosed only under very specific circumstances, primarily in the course of bringing a prosecution for an offence under the Act. The Commissioner and his or her staff are protected against liability for actions done in the course of the exercise of their duties and performed in good faith; this is the usual common law standard.

Decisions and actions of the Commissioner are subject to judicial review but may not be appealed to the courts. The orders of the Commissioner may be filed with a court of competent jurisdiction and treated as orders of that court for enforcement purposes. While failure to comply with an order of the Commissioner is an offence, as discussed below, this allows an effective way of enforcing an order since non-compliance becomes contempt of court.

Whistle-blowing provisions are only recently finding their way into legislation. They recognise that in many cases, only insiders are fully aware of breaches or proposed breaches of the duties and responsibilities that are imposed by legislation, in this case the Policy and proposed Bill to protect personal privacy. For example, the average outsider is unlikely to be aware of whether an organisation (public or private sector) is taking appropriate steps to dispose of personal information—every jurisdiction has stories of health records or bank records being found in alleyways waiting for general garbage collection or personal information being inadvertently faxed or mailed to a third party stranger. Where an organisation fails to respond to internal concerns, the only recourse may be for a person to report breaches of the law to the appropriate authority. The provisions require that there be a reasonable belief that provisions are being breached and that the “whistle-blowing” be done in good faith—this is intended to

protect organisations against retaliation by a disgruntled employee. On the other hand, where such a report has been made, it will be an offence to disadvantage the whistle-blower in any way by dismissal, loss of promotion and so on.

Part III: Principles for Protection of Personal Data by Public Authorities

The provisions relating to the protection of personal data by public authorities are largely drawn from legislation in Canada and Canadian provinces, as well as Australia, New Zealand, the United Kingdom and Ireland. In general, the provisions apply the General Data Protection Principles, but particularize them to the public sector. In a sense, this part might be considered a mandatory code of conduct for public authorities. This Part is mandatory and reflects the fact that public authorities are major collectors and users of personal information.

Certain information is exempted from the definition or concept of "personal information." It is important that citizens and persons dealing with public authorities have access to named individuals and understand what their positions and responsibilities are. The Government, therefore, cannot claim privacy protection to prevent accountability by refusing to connect a named individual with work they've done in the course of their duties for a public authority.

Limitations on protection of personal data about persons who have been dead for more than twenty years are intended to ensure that historical and genealogical research can be conducted and are a compromise between the needs of individuals and historians for this type of information and the privacy interests of the deceased individual.

There are also exceptions with respect to direct collection of information in certain circumstances where it would either be inappropriate to contact the individual directly, it is in the individual's interest that the information be collected, or a larger interest, such as law enforcement, is at stake. The individual is also to be informed of why the information is being collected and, again, there are exceptions to this general requirement. These relate primarily to law enforcement matters or protection of national defence or security. These exceptions are similar to those where access to information may be denied under the *Freedom to Information Act, 1999*.

Where the Government collects information, it is supposed to dispose of it after it has ceased to be of any use. This provision will require co-ordination with the current provisions of the *Freedom of Information Act, 1999*, which forbids the disposal of data. There is an exception to the Policy's requirement for disposal, however. The information should be retained for a sufficient time—some legislation states one year—so that an individual can seek access to the information and correct any inaccuracies if necessary. The Policy and Bill do not state any particular time limit but leave it to the Minister by order to determine appropriate retention periods since this may depend on the nature of the information, the importance of inaccuracies being corrected, the use to which the information was put and so on.

It is in everyone's interest that personal information being held by a public authority be accurate. This places a responsibility on the public authority when collecting the information to use a credible and reliable method of collection. This is also related to the need to maintain security. The degree of attention and care that would be considered reasonable relates to the nature of the information, its sensitivity, the degree of harm that might be caused by inaccuracies, the use to which it is put and other similar considerations.

Protection of personal information relates to physical security, cyber-security and procedures followed by public authorities to ensure the security of the information. The Data Commissioner and others will quite likely need to provide further guidance on appropriate procedures to be followed.

The requirement to maintain storage and access in Trinidad and Tobago is a newer provision that has been placed in legislation following the passage of the *Patriot's Act* in the United States. Under that legislation, if data is held by an organisation that is subject to orders under the *Patriot's Act* (e.g., a U.S. company, the subsidiary of a U.S. company), the data may be released to U.S. authorities; it would be illegal to notify the subject of the inquiry or any other authority. There are already provisions in place for the release of personal information to law enforcement authorities pursuant to international agreements; these arrangements ensure that the law enforcement authorities of Trinidad and Tobago have some control over and knowledge of information being used for law enforcement purposes in other jurisdictions. This appears to be the proper route for seeking such information as opposed to the provisions of the Patriot's Act.

Personal information may be disclosed with the consent of the individual to whom it relates. It may also be disclosed for certain specific purposes, including compliance with a subpoena or warrant or for use in a legal proceeding. It may also be disclosed to law enforcement authorities in another jurisdiction, as noted above, and where there is a compelling reason affecting health and safety. For example, if an individual were infected with an infectious disease, such as avian flu, action could be taken to put in place quarantine and other safety measures even though it might directly or indirectly disclose the identify of the infected person. Public safety would outweigh concerns about personal privacy.

Under certain circumstances personal information may also be disclosed for research or statistical purposes or for archival and historical purposes. These provisions are attempts to balance interests in personal privacy against other needs. The intent is, among other matters, to focus the design of the research to respect personal privacy and ensure that confidentiality safeguards are built into the design and conduct of the research. The Data Commissioner would likely play a role in setting up guidelines for the conduct of research and identifying appropriate safeguards.

The Data Commissioner would also establish guidelines for information sharing agreements among public authorities. Information sharing would not be prohibited, as such, and indeed might be encouraged to reduce the costs of collection. Because sharing might mean that the information was now going to be used for a new purpose or that consent might not have been given to its use, safeguards are required. It is also important that information sharing be adequately documented and the agreements will ensure that this happens.

Data matching may be done within a public authority or may require an information sharing agreement between two or more authorities. Data matching has the potential of yielding new and, to the data subject, unexpected information. Taken to an extreme, it can deliver a detailed snapshot of an individual's life, habits, concerns, and views—in fact, a far more detailed picture than any of us are likely to imagine. On the other hand, it can yield information that allows a public authority to deliver a programme more effectively or can identify non-compliance with public legislation. It is a technique that needs to be used with safeguards, particularly to respect the values of the protection of personal privacy, and the requirement of approval by the Data Commissioner is intended to ensure this. The criteria set out are drawn primarily from the New Zealand legislation and deal with situations where no consent has been given.

If individuals are to take advantage of their right to access (and to correct) their personal information and if public authorities are to be able to respond to requests, then some public index of holdings of personal information is required. Each public authority must annually report to the Data Commissioner on such matters as personal information banks, data sharing agreements, approved data matching agreements, and contact person. Summaries of privacy impact assessments and retention and disposal standards will also be reported. The Data Commissioner will then publish an index of this information. With e-government, this will be an important document to publish electronically and it would be accessible both through the Data Commissioner's website and the website of the Minister responsible for data collection (as well as linked on the websites of the individual public authorities).

Individuals have a basic right to access their personal information held by a public authorities. Individuals are expected to make their requests in writing (which could be electronic) and to provide sufficient information (possibly from the index, above) to allow the public authority to identify and access the information. Any request for an individual's personal information filed under the *Freedom of Information Act, 1999* would be deemed to be a request under this Policy or Bill and subject to this access regime. The head of a public authority could accept an oral request for access if it seemed appropriate.

While generally an individual has the right to access his or her personal information, there are exceptions. In some cases, an individual's information might be so closely inter-twined with another's information that revealing it would

invade the other's privacy. Or the information might be so sensitive that it could prejudice the mental or physical health of the individual, although protocols might be developed that would allow the information to be released by a physician or other professional competent to provide counseling (on such matters as HIV status or genetic testing, for example). Other exceptions relate to such matters as recommendations and evaluations for jobs where they are given in confidence since there is a benefit in encouraging candid evaluations in these circumstances. In addition, there are exemptions relating to such matters as national security or confidences of Cabinet and these are the same as those that are exempted under Part IV of the *Freedom of Information Act, 1999.* The Policy and Bill are thus consistent with that legislation and access to information, personal or otherwise, would be treated the same under both regimes.

In many cases, a sensitive and otherwise exempt piece of information is attached to or part of other information—an exempt sentence or paragraph in an accessible document, for example. The head of the institution should make every effort to ensure that the exempt information is severed from the accessible information and the accessible information provided to the individual making the request. In some cases, for example, excising a name or a section of a document would suffice. The provision should be read generously so that the minimal amount of information is exempted and the individual's right to information is respected to the greatest degree possible.

There are situations, however, where even acknowledging the existence of a document or information provides information that should be exempt. This usually involves a situation dealing with law enforcement or security. For example, stating that information regarding an informant's statements will not be provided confirms that there is an informant. That information alone could endanger the informant. In these situations, a head of a public authority could refuse to even disclose whether or not the information exists.

Although it is expected that most individuals will make requests regarding their own personal information on their own behalf, there are situations where this is impossible. An attorney, executor or legal guardian may make a request on the individual's behalf.

It is not sufficient that individuals merely have access to personal information; it is important that the information be as accurate as possible. Individuals therefore have a right to request correction of information. In some cases, the public authority will accept the new information and make the correction; in other cases, the correction is more a matter of opinion than fact and the authority may decline to make the correction. In that case, the individual may annotate the record with the fact they requested a particular correction and that annotation becomes part of the record.

The individual may appeal to the Data Commissioner about a refusal to provide information or make a correction. The appeal should be filed in writing (which may be electronic) within thirty days of receiving a decision from the head of the public authority. In most cases, the Data Commissioner's first step will be to see if the matter can be mediated. In some situations, a lack of communication or the need to better specify information is behind the dispute. Since the matter involves private information, the mediation or any other investigation may be conducted in private (contrary to the usual provision that dispute settlement involving public authorities is often public, such as in courts or tribunals). There is no formal hearing as such and the matter is not treated as a *lis inter partes*, but the parties may make representations to the Commissioner. To ensure that people can be represented as well as possible, they may use lawyers or other agents or may speak (or write) for themselves. Since the exemptions from disclosure generally involve the interests of government or a government assessment of some broader interest, the burden of proof is on the head of the public authority to argue on the balance of probabilities that the exemption is justified.

In order to deal with appeals or with complaints or other information that may require the Commissioner to investigate and make a determination, the Commissioner has been authorized to make inquiries, require the production of documents, inspect premises and so on. One issue arises with respect to certain public authorities; namely, Parliament and its committees and the courts. These bodies are considered to be public authorities under the *Freedom of Information Act, 1999* and are also defined as public authorities under this Policy and Bill. It is important that they are subject to requirements to protect personal data and respect personal privacy. There is nothing in the General Privacy Principles that should not be applicable to Parliament or the courts. The special status of Parliament and the courts, however, raises an issue with respect to being subject to investigations (e.g., requirements for documents, entry to inspect premises or obtain information) by the Commissioner. The Policy and Bill would deal with this matter by requiring that the Commissioner obtain permission before exercising any investigative powers and thus respect the status of Parliament and the independence of the judiciary. While the exceptions for disclosure would almost certainly cover any "fishing expeditions" into the affairs of Parliament or a case before the courts, it may be advisable to draft a special section to deal with this question. It is not the intention, for example, to interfere with information and documents in cases that are before the courts.

Part IV Principles for Protection of Personal Data by the Private Sector

Part IV establishes a privacy protection regime that is partly voluntary and partly mandatory. Ideally, all persons who collect or hold or use personal information should have systems in place that respect the privacy of the individual whose information they hold. They should protect the information, use it carefully, be sure that it is accurate, dispose of it in a way that does not jeopardize privacy and so on. In some jurisdictions, privacy protection or data protection legislation applies broadly to the private sector with only the smallest of firms exempt from its requirements.

It was decided in Trinidad and Tobago to take a two-pronged approach. The voluntary approach would depend on high visibility, publicity and education about the benefits of good privacy protection practices. The General Privacy Principles are examples of good business practices, but they may require being put into a more detailed and specific form to meet the needs of a particular industries or activities. This is where codes of conduct come in. Codes of conduct have been used widely to implement privacy principles, particularly in New Zealand, Australia, the U.K., Ireland and, to some degree, in Canada. The Data Commissioner would work with industry groups and organisations to provide guidance on the development and content of codes and may, in some circumstances, require that a code of conduct be developed.

Where the Data Commissioner requires an industry or group to develop a code, the intention is that in many cases, this will be a mandatory code. In effect, it will be a set of regulations governing data protection in a particular sector and be tailored to that sector. There are various ways in which this can be accomplished. In some cases, a sectoral regulator may wish to play a lead role in working with industry to develop a code. This might happen, for example, in the financial services industries or the telecommunications industries. The Policy and Bill make provisions for co-operation between sectoral regulators and the Commissioner to ensure that their respective powers do not overlap or clash.

Any code that is intended to be mandatory must be approved by the Commissioner; criteria are provided for the Commissioner to use in his or her considerations. These include not only compliance with the Privacy Principles (which are, after all, the major objective of a code), but also whether the code may have anti-competitive effects. One of the possible weaknesses of codes or any forms of agreements entered into by industries at large is that they may have anti-competitive effects—inadvertently or deliberately. In Australia, the Competition and Consumer Commission must review codes for anti-competitive effects and may in unusual circumstances approve an anti-competitive provision in the larger public interest. In Trinidad and Tobago, there may be future role for such a body, but in the meantime, this matter should be part of the Data Commissioner's considerations.

Where an industry or group develops a code of conduct voluntarily—which is to be encouraged by the Commissioner and the Government at large—it may also ask that the Commissioner approve the code. This would have several benefits for the industry or group: they would have assurance that their code was in compliance with best practices and, in the event of a dispute about their activities, they would have some evidence of having exercised due diligence in such matters as protecting data, gaining consent and following good disposal practices. It may also be a competitive benefit since they could state publicly that their code had been approved.

Where a code is mandatory and therefore has the force of law, an individual may seek a review of a decision or the privacy practices of an organisation by the Data Commissioner. The provisions of Part III of the Policy and Bill apply with any necessary modifications.

Part V: Offences

The general thrust of the Policy and Bill is to encourage good practices with respect to data protection and access to personal information by individuals. The Data Commissioner, for example, has a strong role to play in urging public authorities and private sector organisations to implement good data protection policies and practices and in providing guidance on good practice. It is expected that the Data Commissioner will play a public role educating citizens on their rights and raising the profile of concerns about possible abuses of personal privacy. Voluntary compliance and continuous improvement of data protection practices will be important components of the regime espoused by the Policy and Bill.

There are, however, a few situations in which it is appropriate to mandate behaviour and impose sanctions for lack of compliance. In general, these involve a refusal to comply with orders of the Commissioner or attempts to prevent the Commissioner from carrying out his or her duties and responsibilities. Obstruction, false and misleading information, and failure to comply with orders will all attract sanctions. Similarly, unauthorized disclosure of personal information is an offence: private information cannot be retracted; once it is released, the damage is done. Damages alone may not provide adequate compensation. It is important that this basic underpinning of the Policy be protected with a strong sanction. The exact penalties associated with the offences are yet to be determined but should reflect the potential range of damage and harm and should reflect the different between offences by individuals and offences by corporations. To better encourage compliance by corporations, directors and officers are charged with specific duties to take reasonable care to ensure compliance since studies have shown that the messages regarding compliance given by senior officers and directors of a company have a strong effect on the culture of compliance within the company to the lowest levels. An alternative enforcement mechanism is provided for the orders of the Commissioner: those orders may be filed in a court of competent jurisdiction and will be treated as an order of that court. Consequently, failure to comply with the Commissioner's order will, in effect, be failure to comply with the order of a court and could attract the penalties applicable to contempt of court.