



Data Protection Office

**ICT REGULATORY FRAMEWORK
FROM AN INTERNATIONAL
PERSPECTIVE FOR MAURITIUS**
November 24, 2011
Port Louis, Mauritius



Implementation of data protection: ICT issues

Data Protection is a component of both:

- Electronic commerce
- Delivery of government service


Delivery of services electronically

- Registration applications
- Complaints
- Extracts
- Certificates


Implementation of data protection: ICT issues

Implementation has many implications:


- Ability to collect, analyse and tender electronic evidence
- Criminal activity e.g. 'spoofing,' 'phishing'.



Mauritius
A sugar colony for many years...
Multi-ethnic population comprising the descendants of Indian, African, European and Chinese settlers




Trinidad and Tobago
A sugar colony for many years...
Multi-ethnic population comprising the descendants of Indian, African, European and Chinese settlers



Mauritius

Area 2,040 km²
Pop. (Jul. 2011 est.) 1,286,340
Independence from the UK 12 March 1968




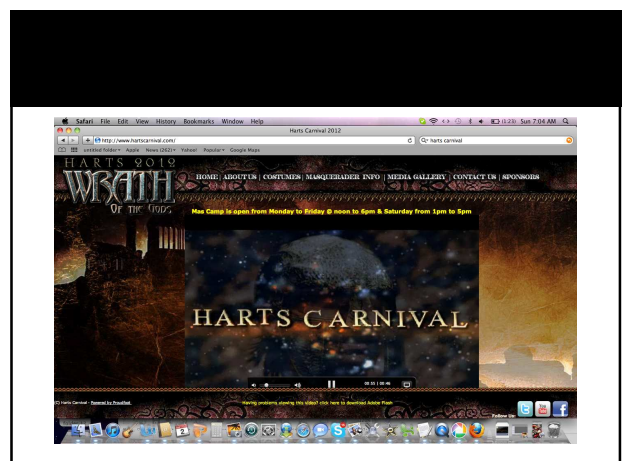
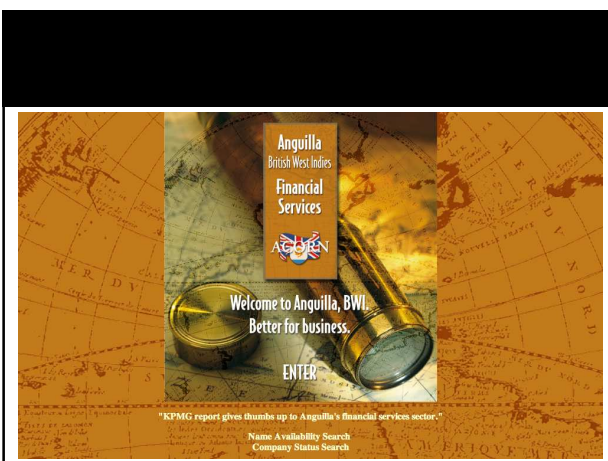
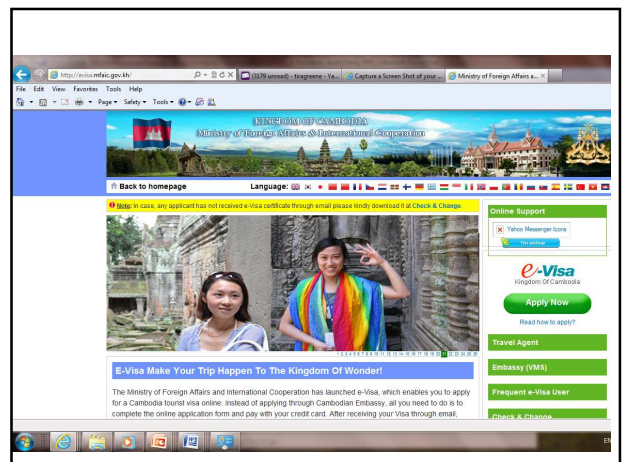
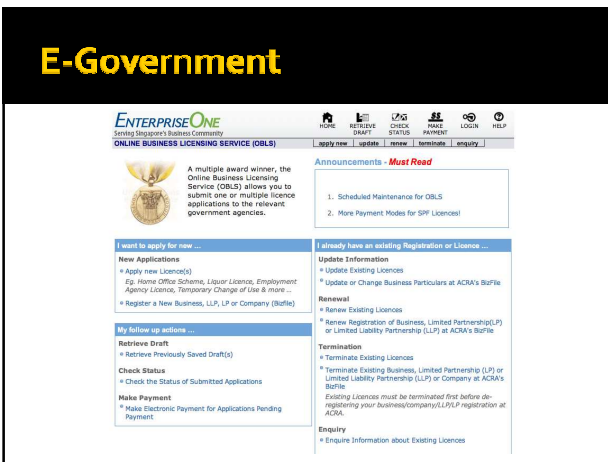
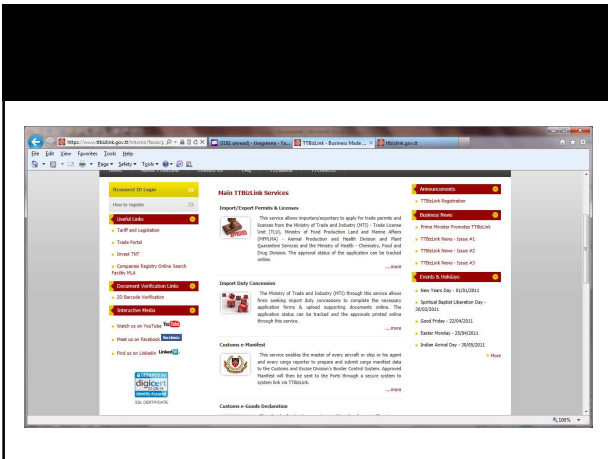
Trinidad and Tobago

Area 5,131 km²
Pop. (Jul. 2011 est.) 1,227,505
Independence from the UK 31 August 1962

Country	GDP (US Billions)	GDP Growth (%)
Mauritius	\$10.986	4.202%
Trinidad and Tobago	\$24.811	2.424%

Source <http://www.economywatch.com/economic-statistics/year/2012/>







ICT Implementation Legislation

- Electronic transactions
- Data protection
- Electronic funds transfer
- Electronic crimes
- Electronic evidence
- Electronic filing

Electronic Transactions Act

- The Act removes legal uncertainties and conflicts and provides for a Commercial Code for the Conduct of Electronic Transactions.
- The Act provides default provisions for contracting in an electronic environment.
- Sec 40 contains an error.

PART XI - PUBLIC SECTOR USE OF ELECTRONIC RECORDS AND SIGNATURES

40. Acceptance of electronic filing and issue of documents
- (1) A public sector agency which, pursuant to any enactment:
- (a) accepts the filing of documents, or requires that documents be created, kept or issued;
 - (b) issues any notice, claim, licence permit, authorisation or approval;
 - (c) provides for any payment and the method and manner of such payment; or
 - (d) has to keep records;

PART XI - PUBLIC SECTOR USE OF ELECTRONIC RECORDS AND SIGNATURES

...may, notwithstanding anything to the contrary in the enactment,

- (i) accept the filing of such documents, or the creation or keeping of such documents in electronic form;
- (ii) issue such notice, claim, licence, permit, authorisation or approval in electronic form;
- (iii) make such payment in electronic form; or
- (iv) convert written records into electronic records.

Electronic Funds Transfer

- The main purpose of this legislation is to regulate the transfer of money by electronic means, by use of a card or number or data associated with a card for the purpose of instructing or authorising a financial institution to debit or credit a cardholder's account when anything of value is purchased.
- A number of offences need to be created related to the theft, forgery and other dishonest use of a credit card, debit card, bank card, smart card, or the number and data associated with such card or a bank account, and is intended to build user confidence in electronic commerce and electronic transfers.

Electronic Crimes Legislation

- Electronic crime includes monetary offences as well as non-monetary offences such as creating and distributing viruses on other computers, sending threats via email or posting libelous information on the Internet.
- Offences need to be created for specific crimes.
- These new technology-enabled crimes require that new procedural powers be given to law enforcement authorities to effectively investigate and prosecute the commission of such crimes.

Electronic Crimes Legislation

The Computer Misuse and Cybercrime Act 2003 created a number of offences:

- Unauthorised access to computer data
- Access with intent to commit offences
- Unauthorised access to and interception of computer service
- Unauthorised modification of computer material
- Damaging or denying access to computer system
- Unauthorised disclosure of password
- Unlawful possession of devices and data
- Electronic fraud

Electronic Crimes

Since 2003 electronic crimes have become more diverse, as have case law and the legislation to deal with them. Examples of these crimes are:

- Invasion of privacy
- Spoofing (e.g. "phishing")
- Malicious code
- Cyber-stalking
- Cyber-terrorism
- Sending offensive messages through communication services, etc.
- Identity theft

Implementation of data protection: Electronic Evidence

The issue of admissibility and evidential weight of electronic records in court proceedings is important and not adequately covered under existing evidence laws.

New legislation should make provision for legal recognition of electronic records to facilitate the admission of such records into evidence in legal proceedings.

Electronic Evidence

Countries such as Singapore and Canada have amended their evidence legislation to give legal recognition to electronic records and electronic signatures by way of evidentiary presumptions to ensure these have the same legal effect, validity or enforceability as paper records.

Electronic Evidence

These presumptions are:

- There is no legal difference between electronic records and paper records.
- There is no legal difference between electronic records and paper documents when satisfying the legal requirements of being in writing.
- There is no legal difference between an electronic signature and a hand-written signature when satisfying the legal requirement of a signature.

Electronic Evidence

Presumptions cont'd...

- There is no legal difference between electronic records and paper records when admitting these as evidence in legal proceedings.
- There is no legal difference between a contract entered into electronically and a paper contract.
- There is no legal difference between an electronic signature and a hand-written signature when satisfying the legal requirement of a signature.

Electronic Evidence

Presumptions cont'd...

- There is no legal difference between electronic records and paper records when admitting these as evidence in legal proceedings.
- There is no legal difference between a contract entered into electronically and a paper contract.

Electronic Evidence

The storage of electronic evidence, very often in disk files not known to the creator of the electronic evidence, may actually make it easier to rebut or corroborate the evidence.

It is also technically more difficult to totally delete "unwanted" electronic evidence and tampering with such evidence also results in electronic "footprints".

Electronic Filing Rules

The purpose of electronic filing legislation is to add electronic delivery to the existing list of approved methods of document delivery and fee payment within the public sector.

The provisions should aim to:

- Authorize electronic filing;
- Define the electronic filing system; and
- Specify the procedural mechanics.

Thank You

Presented by: Tira Greene

E-mail: tiragreene@yahoo.com