Regional Conference on Policies and Strategies on cybercrime for the Caribbean Community

Legal Framework on Cybercrime and Electronic Evidence

Santo Domingo – 12 June 2019

Cybercrime legislation

- **1984 United States Computer Fraud and Abuse Act from 1984,** introduces legislation against the CIA triad although in a limited fashion to acts against protected computer which are those used by the Federal Government and certain financial institutions.
- **1988 French Loi Godfrain** protects all computer systems against breaches of the confidentiality, integrity, accessibility.
- **2001 Budapest Convention**, and international legal instrument requiring signatory countries to have certain minimum offenses.

What else is needed outside of the Budapest convention

- **Can an old law cover todays cybercrime**? French constitutional review (QPC) of 10 April 2013 (12-85.618) found that the articles are sufficiently clear and precise for their interpretation and their sanctions, who belong to the judge in criminal matters, can be made without risk of an arbitrary sentence.
- **Spam legislation**: no agreement during the Budapest Convention drafting between opt-in and opt-out. Nonetheless, most countries have separate national legislation dealing with unsolicited electronic communications.
- **Personal data legislation**. Limiting the use of personal data to when it is needed such as: by consent, because of the need to complete a commercial relationship, legal obligation, vital interest of the data subject, processing for public interest, or legitimate interest.
- **Identity theft**: French article 226-4-1: using the identity of a third party or information allowing the identify a third party with the purpose to trouble his peace, or that of others, or to damage their honor or reputation, is punished with a prison term of one year and a fine of 15 000€.
- **Phishing**. Rarely legislated as Misuse of Devices can be used for criminalizing preparatory steps from Phishkits as well as the procurement of the password. Trademark legislation has also been used by brand owners when the phishing page abuses their brand to commit the phishing.

The Council of Europe Convention on Cybercrime

The approach of Council of Europe

1 Common standards: Budapest Convention on Cybercrime and related standards

2 Follow up and assessments: Cybercrime Convention Committee (T-CY)

3 Capacity building: C-PROC ▶ Technical cooperation programmes

Budapest Convention: scope

Criminalising conduct

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

+

Procedural tools

- Expedited preservation
- Partial disclosure of traffic data
- Production orders
- Search and seizure
- Interception of computer data

+

International cooperation

- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

Harmonisation

Substantive Criminal Law

Substantive provisions:

- Illegal **access**
- Illegal **Interception**
- Data **Interference**
- System **Interference**
- **Misuse** of Devices
- Computer **Forgery** & **Fraud**
- Child Pornography
- Intellectual Property Rights
- **Aiding/Abetting**
- **Corporate Liability**

Illegal Access

Computer / Data / Program

Article 2 – Illegal access

*Each Party **shall** adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, **when committed intentionally, the access to the whole or any part of a computer system without right.***

*A Party **may** require that the offence be committed by **infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system** that is connected to another computer system.*

Article 3 – Illegal interception

*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed **intentionally**, the **interception without right**, made by **technical means**, of **non-public transmissions** of computer data **to**, **from** or **within** a **computer system**, including **electromagnetic emissions** from a computer system carrying such computer data. A Party may require that the offence be committed with **dishonest intent**, or **in relation to a computer system that is connected to another computer system**.*

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the ***damaging, deletion, deterioration, alteration or suppression*** *of computer data* ***without right****.*

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the ***serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.***

Article 6 – Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the ***production, sale, procurement for use, import, distribution*** *or otherwise* ***making available*** *of:*

i a ***device, including a computer program****, designed or adapted* ***primarily*** *for the purpose of committing any of the offences established in accordance with Articles 2 through 5;*

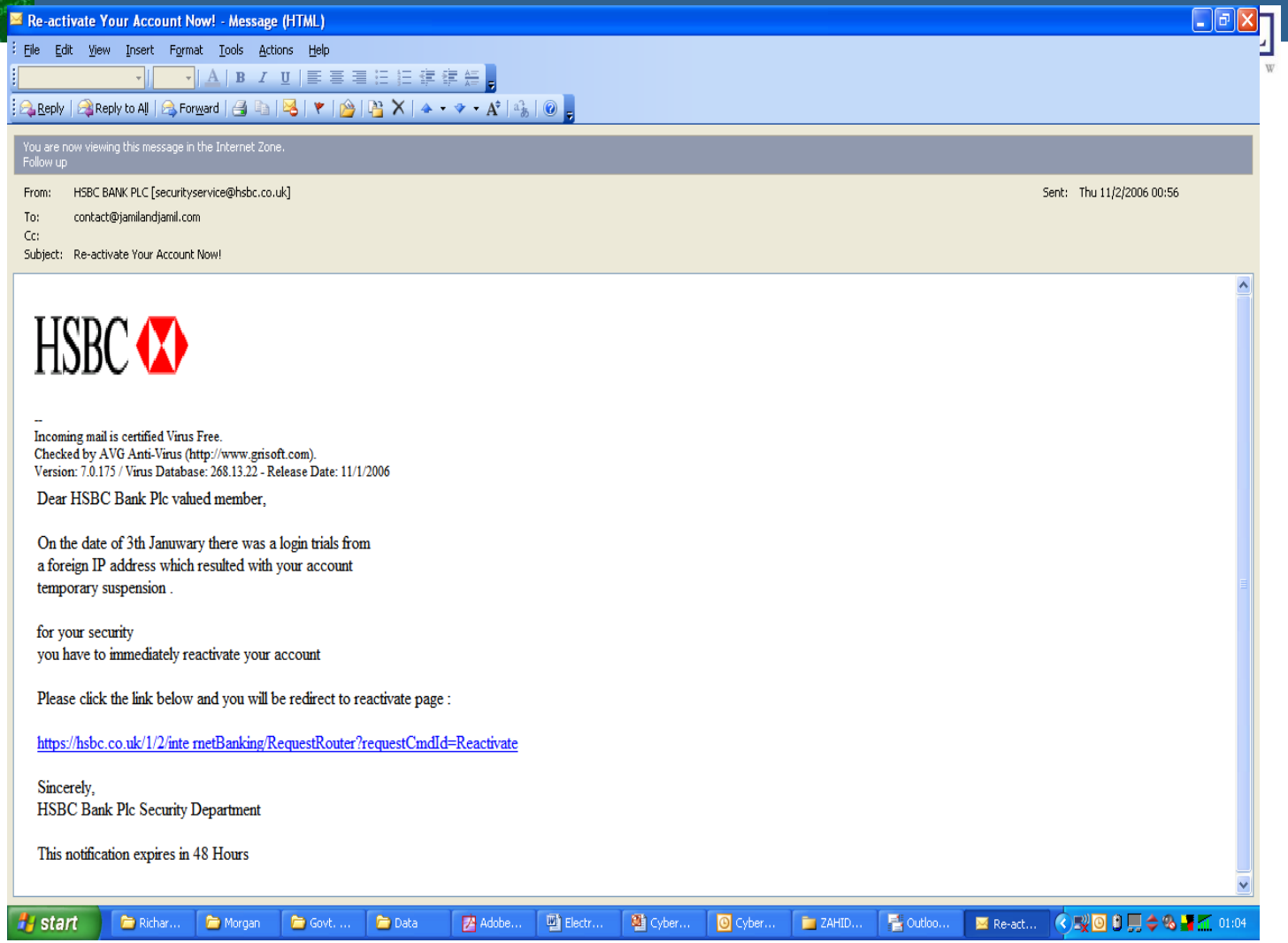
ii a ***computer password, access code, or similar data*** *by which the whole or any part of a computer system is capable of being accessed,*

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

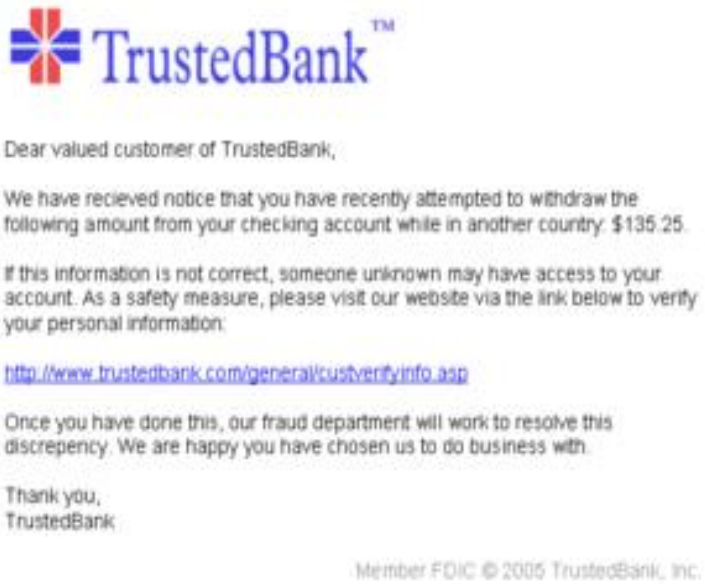
b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

*2 This article shall **not be interpreted as imposing criminal liability where** the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is **not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention**, such as for the authorised testing or protection of a computer system.*

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.


Re-activate Your Account Now! - Message (HTML)
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward
You are now viewing this message in the Internet Zone.
Follow up
From: HSBC BANK PLC [securityservice@hsbc.co.uk]
Sent: Thu 11/2/2006 00:56
To: contact@jamilandjamil.com
Cc:
Subject: Re-activate Your Account Now!
HSBC
--
Incoming mail is certified Virus Free.
Checked by AVG Anti-Virus (http://www.grisoft.com).
Version: 7.0.175 / Virus Database: 268.13.22 - Release Date: 11/1/2006
Dear HSBC Bank Plc valued member,
On the date of 3th Januwary there was a login trials from
a foreign IP address which resulted with your account
temporary suspension .
for your security
you have to immediately reactivate your account
Please click the link below and you will be redirect to reactivate page :
https://hsbc.co.uk/1/2/inte rnetBanking/RequestRouter?requestCmdId=Reactivate
Sincerely,
HSBC Bank Plc Security Department
This notification expires in 48 Hours
start
Richar...
Morgan
Govt. ...
Data
Adobe...
Electr...
Cyber...
Cyber...
ZAHID...
Outloo...
Re-act...
01:04

Phishing



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

SUNTRUST

-----Original Message-----
From: SunTrust Bank [mailto:clientserviceteam.refaz97178839404.nf@suntrust.com]
Sent: Wednesday, July 11, 2007 1:00 AM
To:
Subject: SunTrust Bank Client Service Team: Customer Alert!

Dear SunTrust Bank customer,

SunTrust Client Service Team requests you to complete Online Treasury Customer Form.

This procedure is obligatory for all business and corporate clients of SunTrust Bank.

Please click hyperlink below to access Online Treasury Customer Form.

http://onlinetreasurymanager-id66744585.suntrust.com/ibswebsuntrust/cmserver/customer.cfm

Thank you for choosing SunTrust Bank for your business needs.

Please do not respond to this email.

This mail generated by an automated service.

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed ***intentionally*** *and* ***without right****, the input, alteration, deletion, or suppression of computer data, resulting in* ***inauthentic data*** *with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.*

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the ***causing of a loss of property to another person*** *by:*

a any input, alteration, deletion or suppression of computer data,

b any interference with the functioning of a computer system,

with ***fraudulent or dishonest intent*** *of* ***procuring****, without right, an* ***economic benefit for oneself or for another person****.*

Article 9 – Offences related to child pornography

1. *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:*

*a) **producing** child pornography for the purpose of its distribution through a computer system;*

*b) **offering** or **making available** child pornography through a computer system;*

*c) **distributing** or **transmitting** child pornography through a computer system;*

*d) **procuring** child pornography through a computer system for oneself or for another person;*

*e) **possessing** child pornography in a computer system or on a computer-data storage medium.*

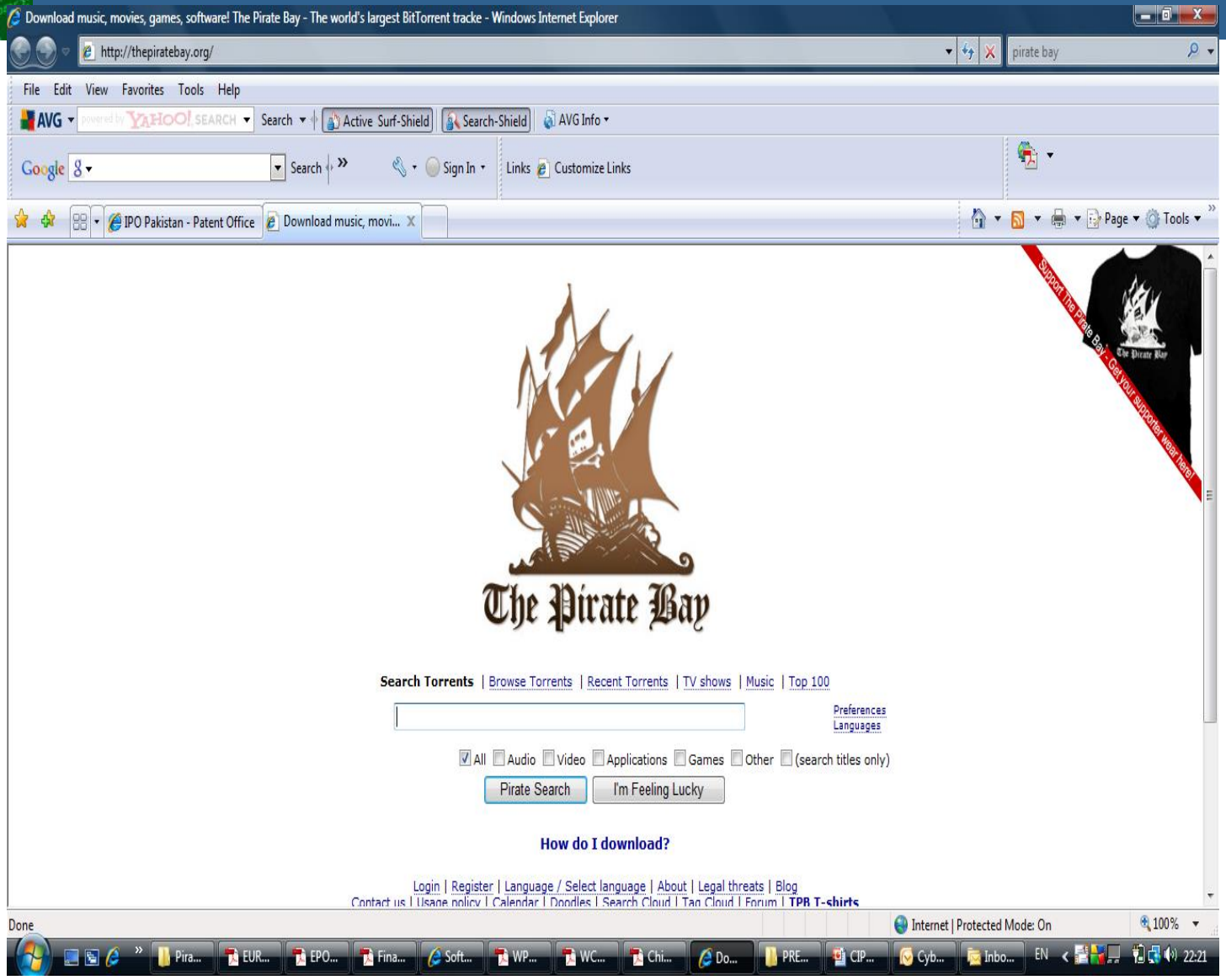
*2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that **visually depicts:***

a) a minor engaged in sexually explicit conduct;

*b) a person **appearing to be a minor** engaged in sexually explicit conduct;*

*c) **realistic images** representing a minor engaged in sexually explicit conduct.*

3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.


Download music, movies, games, software! The Pirate Bay - The world's largest BitTorrent tracke - Windows Internet Explorer
http://thepiratebay.org/
pirate bay
File Edit View Favorites Tools Help
AVG Search Active Surf-Shield Search-Shield AVG Info
Google Search Sign In Links Customize Links
IPO Pakistan - Patent Office
Download music, movi...
Page Tools
Support The Pirate Bay - Get your supporter wear here!
The Pirate Bay
Search Torrents | Browse Torrents | Recent Torrents | TV shows | Music | Top 100
Preferences
Languages
All Audio Video Applications Games Other (search titles only)
Pirate Search
I'm Feeling Lucky
How do I download?
Login | Register | Language / Select language | About | Legal threats | Blog
Contact us | Usage policy | Calendar | Doodles | Search Cloud | Tag Cloud | Forum | TPB T-shirts
Done
Internet | Protected Mode: On
100%
22:21

Article 10 – Offences related to infringements of copyright and related rights

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, ***pursuant to the obligations it has undertaken under*** *the* ***Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty****, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.*

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, ***pursuant to the obligations it has undertaken under*** *the* ***International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty****, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.*

Procedural Law

Article 15 § 1
Conditions and safeguards

1. *"Each Party shall ensure that the **establishment, implementation and application** of the powers and procedures provided for in (Art. 14 to 21) are **subject to conditions and safeguards** provided for under its **domestic law** (…)".*
2. *These safeguards must "provide for the adequate protection of human rights and liberties, **including rights arising pursuant to obligations it has undertaken** under applicable international human rights instruments (inter alia the 1950 Council of Europe "European Convention of Human Rights" and the 1966 United Nations International Covenant on Civil and political Rights).*

Conditions and safeguards under European Convention of Human Rights

Conditions to be met when limiting rights:

- Exclusive competence of the law (legal basis)
- Need to pursue a legitimate aim (**l**egitimate aim)
- “Necessity of the interference in a democratic society”... which means that the interference must:
  - correspond to a "pressing social need“ (**necessity**)
  - be proportionate to the aim pursued (**proportionality**)
- Requirements implied by the “necessity” and “proportionality” principles might be classified under the one or the other notion.

Article 16 – Expedited Preservation of Stored Computer Data

1. *Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the **expeditious preservation** of **specified computer data**, including traffic data, that has been **stored** by means of a computer system, in particular where there are grounds to believe that the computer data is **particularly vulnerable to loss or modification**.*

Article 16 – Expedited Preservation of Stored Computer Data

2. *Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and* ***maintain the integrity*** *of that computer data for a period of time* ***as long as necessary****, up to a* ***maximum of ninety days****, to enable the competent authorities to* ***seek its disclosure****. A Party may provide for such an order to be* ***subsequently renewed****.*

Article 16 – Expedited Preservation of Stored Computer Data

3. *Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to **keep confidential the undertaking of such procedures** for the period of time provided for by its domestic law.*

4. *The powers and procedures referred to in this article shall be **subject to Articles 14 and 15**.*

Article 17 – Expedited Preservation of Partial Disclosure of Traffic Data

1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

*a) ensure that such **expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission** of that communication; and*

*b) ensure the **expeditious disclosure** to the Party's competent authority, or a person designated by that authority, of a **sufficient amount of traffic data** to enable the Party to **identify the service providers and the path** through which the communication was transmitted.*

Article 18 - Production Order

1. *Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:*

   a) ***a person in its territory*** *to submit* ***specified computer data*** *in that person's* ***possession or control****, which is stored in a computer system or a computer-data storage medium; and*

   b) ***a service provider offering its services in the territory*** *of the Party to submit* ***subscriber information*** *relating to such services in that service provider's* ***possession or control****.*

2. *The powers and procedures referred to in this article shall be* ***subject to Articles 14 and 15****.*

Article 18 - Production Order

3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a) the type of communication service used, the technical provisions taken thereto and the period of service;

b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Article 19 -
Search and Seizure of Stored Computer Data

1. *Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to **search or similarly access**:*

   a) *a **computer system** or **part of it** and **computer data stored** therein; and*

   b) *a **computer-data storage medium** in which computer data may be stored in its territory*

Article 19 - Search and Seizure of Stored Computer Data

2. *Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have* ***grounds to believe that the data sought is stored in another computer system*** *or part of it in its territory, and such data is* ***lawfully accessible from or available to the initial system****, the authorities shall be able to* ***expeditiously extend the search or similar accessing*** *to the other system.*

Article 19 -
Search and Seizure of Stored Computer Data

*3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to **seize or similarly secure** computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:*

a) ***seize or similarly secure*** *a computer system or part of it or a computer-data storage medium;*

b) ***make and retain a copy*** *of those computer data;*

c) ***maintain the integrity*** *of the relevant stored computer data;*

d) ***render inaccessible or remove*** *those computer data in the accessed computer system.*

Article 19 - Search and Seizure of Stored Computer Data

4. *Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to* ***order any person who has knowledge about the functioning of the computer system*** *or* ***measures applied to protect the computer data*** *therein to* ***provide,*** *as is reasonable, the* ***necessary information,*** *to enable the undertaking of the measures referred to in paragraphs 1 and 2.*

Real-time Collection of Traffic Data

(Article 20 – Budapest Convention)

- Allows alive investigations
- Intrusive measure, requires proper legislation
- Law enforcement authorities to collect or record, through technical means, data in real time, and
- Power to compel service providers to collect or record data from their costumers, in real time.

Article 20
Real-time Collection of Traffic Data

1. *Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:*

   a) ***collect or record*** *through the application of* ***technical means*** *on the territory of that Party, and*

   b) ***compel a service provider, within its existing technical capability:***

      I. ***to collect or record*** *through the* ***application of technical means*** *on the territory of that Party; or*

      II. ***to co-operate*** *and assist the* ***competent authorities*** *in the collection or recording of,*

   traffic data*, in* ***real-time,*** *associated with* ***specified communications*** *in its territory transmitted by means of a computer system.*

Article 20
Real-time Collection of Traffic Data

2. *Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.*

Article 20
Real-time Collection of Traffic Data

3. *Each Party shall adopt such legislative and other measures as may be necessary to **oblige a service provider to keep confidential** the fact of the execution of any power provided for in this article and any information relating to it.*

3. *The powers and procedures referred to in this article shall be **subject to Articles 14 and 15**.*

Article 21
Interception of Content Data

1. *Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of **serious offences** to be determined by domestic law, to empower its competent authorities to:*

   a) ***collect or record*** *through the* ***application of technical means*** *on the territory of that Party, and*

   b) ***compel a service provider****, within its* ***existing technical capability:***

      I. ***to collect or record*** *through the application of* ***technical means*** *on the territory of that Party, or*

      II. ***to co-operate*** *and assist the* ***competent authorities*** *in the collection or recording of,*

   content data*, in* ***real-time****, of* ***specified communications*** *in its territory transmitted by means of a computer system.*

Article 21
Interception of Content Data

2. *Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.*

Article 21
Interception of Content Data

3. *Each Party shall adopt such legislative and other measures as may be necessary to **oblige a service provider to keep confidential** the fact of the execution of any power provided for in this article and any information relating to it.*

4. *The powers and procedures referred to in this article shall be **subject to Articles 14 and 15**.*

Questions