Funded by the European Union and the Council of Europe
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Implemented by the Council of Europe

Introductory Judicial Training Course on Cybercrime and Electronic Evidence

Substantive Provisions of the Budapest Convention & Analogous Provisions of the Malabo Convention - Part 2

Jennifer Mensah (Mrs.)
Cybersecurity and Data Privacy Legal Practitioner
National Communications Authority, Ghana
Council of Europe

email

9th November, 2021

Session contents

1. Computer-related forgery
2. Computer-related fraud
3. Child pornography
4. Infringement of copyright and related rights
5. Ancillary Liability

Session aim

- To provide the participants with a comprehensive understanding of the elements of computer-related offences, content-related offences and offences related to the infringement of copyright and related rights, established in accordance with the Budapest Convention.

Session objectives

By the end of the session, delegates will be able to:

Identify the elements which constitute the offence of:

- Computer-related forgery
- Computer-related fraud
- Child pornography
- Infringement of copyright and related rights

Understand how the Budapest Convention criminalizes aiding, abetting and attempting offences, and the scope of corporate liability

Substantive Provisions of the Budapest Convention (Part 2)

COMPUTER-RELATED FORGERY

Computer-related forgery

Computer-related Forgery

(Art. 7 – Budapest Convention)

- *Creates parallel offence to forgery of tangible offences*
- *Gap in criminal law as traditional forgery usually requires visual readability of statements or declarations embodied in document*
- *Traditional forgery may not apply to electronic data*

Computer-related forgery ("input, alteration...")

- 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.

- The scope of this offence is limited to the falsification of documents by:
  - Input of correct or incorrect data
  - Subsequent alteration (modifications, variations, partial changes)
  - Deletion (removal of data from a data medium)
  - Suppression (holding back, concealment of data)

Malabo Convention Computerized Data Breaches (Art 29 (2b))

State Parties shall take the necessary legislative and/or regulatory measures to make it a criminal offence to :

- 2b: intentionally input, alter, delete or suppress 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 of whether or not the data is directly readable or intelligible. A party may require an intent to defraud or similar dishonest intent before criminal liability attaches

Computer-related forgery: Example

DELHI

Doctor, aide arrested for giving forged COVID-19 test reports

STAFF REPORTER

NEW DELHI , SEPTEMBER 04, 2020 22:47 IST
UPDATED: SEPTEMBER 04, 2020 22:47 IST

Police act on complaint from lab

A 34-year-old doctor and his associate have been arrested for allegedly preparing forged COVID-19 test reports, police said on Friday.

Deputy Commissioner of Police (South) Atul Thakur said the accused had been identified as Dr. Kush Bihari Parashar and his associate Amit Singh. They had forged at least 75 reports.

Police said they received a complaint on August 30 from a noted testing lab in Hauz Khas regarding forgery of a COVID-19 report with their centre's name on it. Based on the complaint, a case on charges of cheating, forgery and fraud was registered.

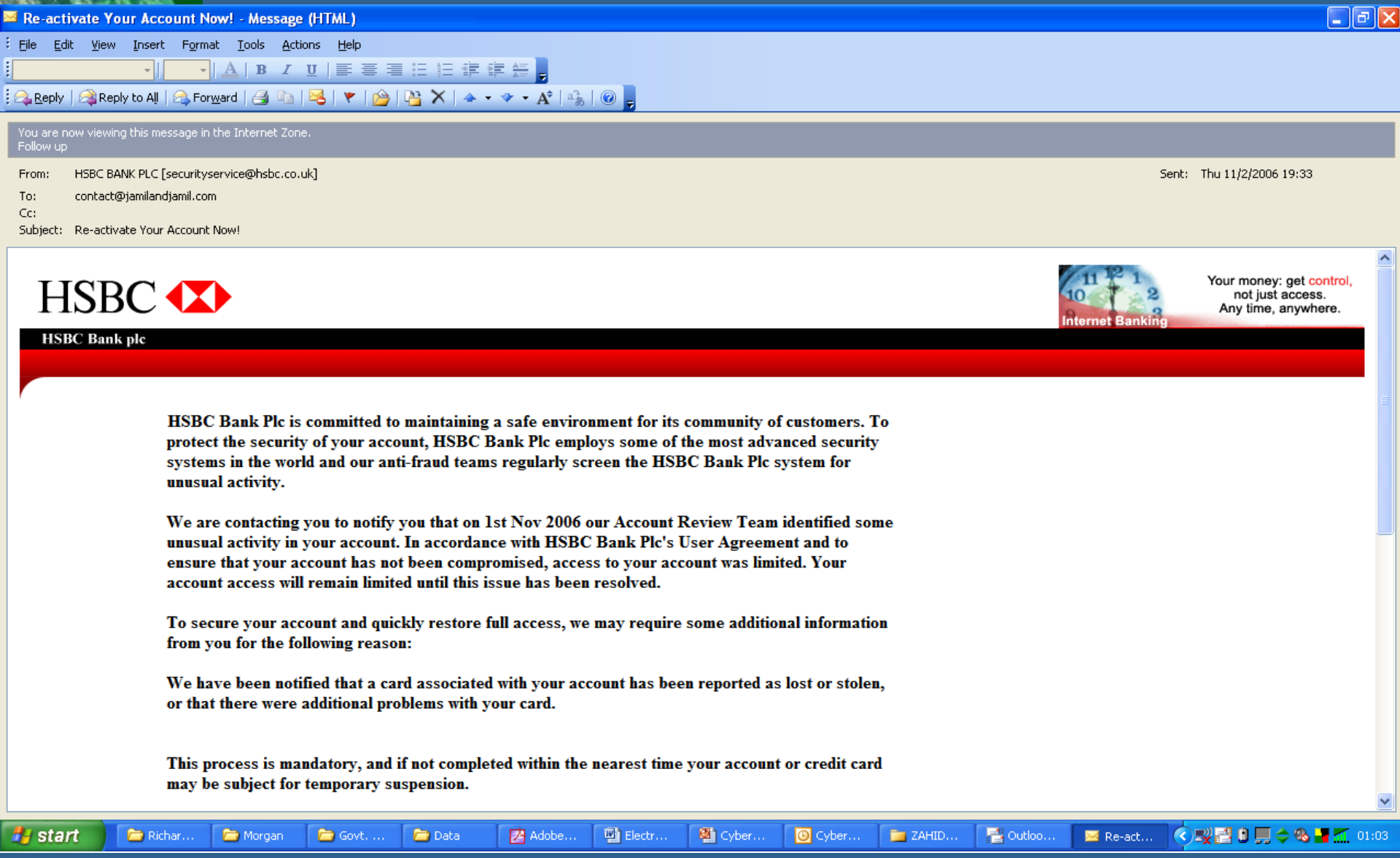
Police said a person who ran a business of providing nursing staff to people asked Dr. Parashar for COVID-19 tests of his two nurses before they were hired. The doctor sent the reports to the person on WhatsApp in PDF format who further sent the reports to his client who wanted to hire the nurse.

The client spotted a mistake in the name and contacted the testing lab straight for her query on the name and asked them to send a new report with corrected name. The lab stated that they had no record of testing the nurse.

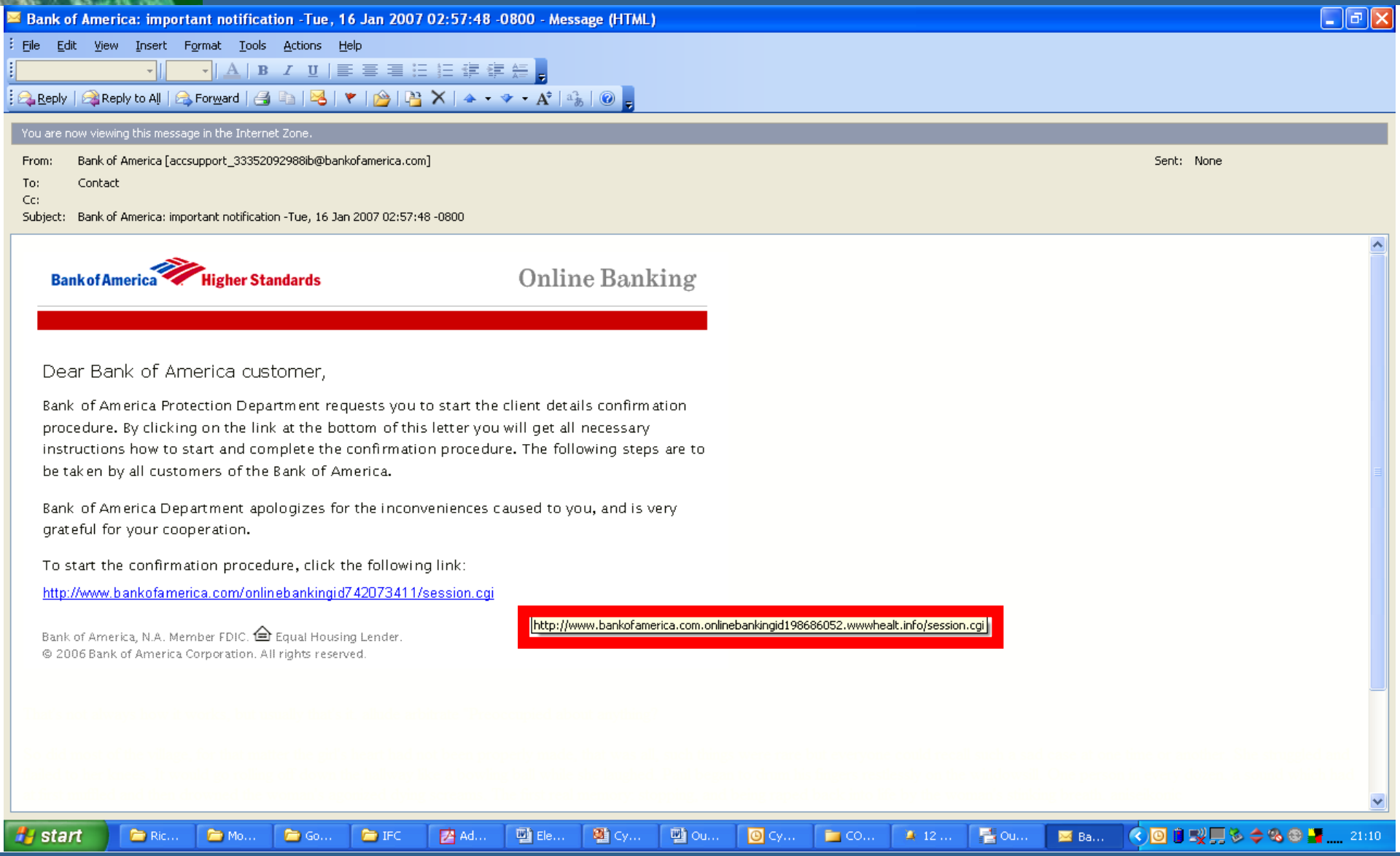
During investigation, it was found that the doctor would recommend people for COVID-19 testing after which he would collect the sample himself or his associate Amit would. The duo wouldn't send the samples for testing and make forged test reports of centres which the patients desired, police said. "As the reports were prepared in PDF format on computer and same were sent to patients on WhatsApp, it was difficult to differentiate between the forged and the genuine report," Mr. Thakur said.

The doctor, police said, was charging ₹2,400 a test.

Computer-related forgery: Example



Computer-related forgery: Example



Computer-related forgery ("input, alteration...")

- 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.

- The scope of this offence is limited to the falsification of documents by:
  - Input of correct or incorrect data
  - Subsequent alteration (modifications, variations, partial changes)
  - Deletion (removal of data from a data medium)
  - Suppression (holding back, concealment of data)

Computer-related forgery ("inauthentic data")

- 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.

- Ordinarily, the term authenticity relates to:
  - Authenticity as to the author of a document
  - Authenticity as to the truthfulness of the statement contained in the document

- Authenticity in relation to data at a minimum refers to the issuer of the data (regardless of the correctness/veracity of its contents)

- Authenticity may also optionally relate to the genuineness of the data

Computer-related forgery ("intent that it be…")

- 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.

- Additional intent requirement

- "for legal purposes" includes legal transactions and documents which are legally relevant

Computer-related forgery ("regardless…directly readable…")

- 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.

- The inauthentic data does not necessarily have to be directly readable or intelligible by a human being

Computer-related forgery ("intent to defraud...")

- 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.

- ✓ Parties may limit the criminalization of computer-related forgery with the following qualifying elements:
  - ✓ Intent to defraud
  - ✓ Dishonest intent

Substantive Provisions of the Budapest Convention (Part 2)

COMPUTER-RELATED FRAUD

Computer-related fraud

Computer-related Fraud

(Art. 8 – Budapest Convention)

- *Creates parallel offence to fraud related to tangible offences*

Computer-related fraud: Example

Kenya Revenue Authority 'lost $39m to hacker'

22 March 2017

Alex Mutuku's lawyers want him to be released on bail

An IT expert has been charged with hacking into Kenya's Revenue Authority and stealing $39m (£31m).

Alex Mutungi Mutuku, 28, is accused of electronic fraud but he denies any wrongdoing.

The prosecution says he is part of an international network stealing money from several state bodies.

The government says there is a ring involving expatriates from the United States and other countries, along with police officers and civil servants.

A thorough background check on state employees is now being conducted, government spokesperson Eric Kiraithe told the BBC.

'Tip of the iceberg'

He is being held while anti-cybercrime officers dig deeper into what they believe is an elaborate fraud scheme with international connections.

It allegedly involves hackers with access to high-tech equipment and software which enabled them to steal from corporations, Kenya's Standard newspaper reports.

"It is a case of remote control hacking where the suspects operate smoothly with their machines and the next minute you realise you have no money in your account," state prosecutor Edwin Okello is quoted by the newspaper as saying.

"The information we have is just a tip of the iceberg. The racket is big and involves people outside the country."

The cybercrime unit says Kenya lost $165m (£132m) through hacking in 2016.

Earlier this month, several people including foreign nationals were arrested in Nairobi over their involvement in theft of funds through hacking.

Ten suspects have so far been charged in court.

Computer-related fraud ("input, alteration, deletion...")

- 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**,

  a) 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.

- The scope of this offence is limited to causing loss of property to another person by:

  - Input of correct or incorrect data
  - Subsequent alteration (modifications, variations, partial changes)
  - Deletion (removal of data from a data medium)
  - Suppression (holding back, concealment of data)
  - Interference with the functioning of a computer system

Computer-related fraud ("loss of property")

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

  a) 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.

- The act of computer-related fraud must produce direct economic or possessory loss of another person's property

- This would include loss of:
  - Money
  - Tangibles
  - Intangibles with an economic value

Computer-related fraud ("fraudulent… dishonest…")

- 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,

  a) 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**.

- Additional intent requirement

- The act must be committed by the perpetrator with the intent of procuring unlawful gain for himself or for another person

MALABO CONVENTION: Article 29 (2d)

- State Parties shall take the necessary Legislative and/or regulatory measures to make it a criminal offence to:

2d: Fraudulently procure, for oneself or for another person, any benefit by inputting, altering, deleting or suppressing computerized data or any other form of interference with the functioning of a computer system.

Poll question

A company inputs data on its website identifying benefits of its product over a competitor's product. This causes economic benefit to the company and loss of property to the competitor.

Is this an offence under Article 8 of the Budapest Convention?

a) Yes

b) No

Poll question

A company inputs data on its website identifying benefits of its product over a competitor's product. This causes economic benefit to the company and loss of property to the competitor.

Is this an offence under Article 8 of the Budapest Convention?

a) Yes

b) No

Substantive Provisions of the Budapest Convention (Part 2)

ONLINE CHILD SEXUAL EXPLOITATION

Child pornography

Child Pornography (Article 9 – Budapest Convention)

- *Great innovation*
- *Criminalisation of child pornography acts, committed by means of a computer system*
- *Important aspects:*
  - *Criminalisation of "pseudo images";*
  - *Punishment of the mere possession of child pornography materials*
    - *Not covered by many of the legislations*
    - *Very common approach from all the international fora (eg. UN)*
    - *European Union*
      - *Enfaces the mere possession of child pornography materials*
      - *Directive 2011/92/EU, from the European Parliament and the Council*

Child pornography: Example

43 arrested in anti-child porn operation in Brazil

19 arrests, the largest number, were made in Sao Paulo, the most populous state in Brazil, followed by Santa Catarina with nine, and Parana with six.

IANS | Brasilia | February 19, 2020 12:47 pm

Brazil police have arrested 43 people in a large-scale operation against child pornography which involved four other countries.

According to the Brazilian authorities, 112 search warrants were issued in the sixth phase of the Federal Police's Childhood Light Operation, with the participation of 579 law enforcement officers.

The warrants were executed on Tuesday in 12 Brazilian states, including Sao Paulo, Santa Catarina, Parana and Mato Grosso do Sul, Xinhua news agency reported.

19 arrests, the largest number, were made in Sao Paulo, the most populous state in Brazil, followed by Santa Catarina with nine, and Parana with six.

Law enforcement agencies in the United States, Colombia, Panama and Paraguay were also involved in the operation and executed warrants in their territories.

According to the police, the 43 people were arrested on accusations such as production, possession and distribution of child pornography. Sentences for each of those crimes can be up to eight years in prison.

Over 187,000 files were seized for analysis, which may lead to other phases of the Childhood Light Operation. A total of 640 arrests have been made since the first edition of the operation was launched in 2017.

Child pornography: Example

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Wednesday, October 16, 2019

South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin

Dozens of Minor Victims Who Were Being Actively Abused by the Users of the Site Rescued

Jong Woo Son, 23, a South Korean national, was indicted by a federal grand jury in the District of Columbia for his operation of Welcome To Video, the largest child sexual exploitation market by volume of content. The nine-count indictment was unsealed today along with a parallel civil forfeiture action. Son has also been charged and convicted in South Korea and is currently in custody serving his sentence in South Korea. An additional 337 site users residing in Alabama, Arkansas, California, Connecticut, Florida, Georgia, Kansas, Louisiana, Maryland, Massachusetts, Nebraska, New Jersey, New York, North Carolina, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, Texas, Utah, Virginia, Washington State and Washington, D.C. as well as the United Kingdom, South Korea, Germany, Saudi Arabia, the United Arab Emirates, the Czech Republic, Canada, Ireland, Spain, Brazil and Australia have been arrested and charged.

Assistant Attorney General Brian A. Benczkowski of the Justice Department's Criminal Division, U.S. Attorney Jessie K. Liu for the District of Columbia, Chief Don Fort of IRS Criminal Investigation (IRS-CI) and Acting Executive Associate Director Alysa Erichs of U.S. Immigration and Customs Enforcement (ICE)'s Homeland Security Investigations (HSI), made the announcement.

"Darknet sites that profit from the sexual exploitation of children are among the most vile and reprehensible forms of criminal behavior," said Assistant Attorney General Brian A. Benczkowski of the Justice Department's Criminal Division. "This Administration will not allow child predators to use lawless online spaces as a shield. Today's announcement demonstrates that the Department of Justice remains firmly committed to working closely with our partners in South Korea and around the world to rescue child victims and bring to justice the perpetrators of these abhorrent crimes."

"Children around the world are safer because of the actions taken by U.S. and foreign law enforcement to prosecute this case and recover funds for victims," said U.S. Attorney Jessie K. Liu. "We will continue to pursue such criminals on and off the darknet in the United States and abroad, to ensure they receive the punishment their terrible crimes deserve."

Child pornography ("without right")

- 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.

- There may be legal defences, excuses or similar relevant principles that relieve a person of criminal liability

- These defences may be based on the freedom of expression, freedom to thought and right to privacy

- Parties may also allow a defence in relation to pornographic materials having artistic, medical, scientific or similar merit

Child pornography ("producing… offering…")

- 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.

- ✓ Criminal consequences attached to each participant in chain from production to possession of child pornography

- ✓ Criminalizes:
  - ✓ Production of child pornography (for the purpose of distribution by means of computer system)
  - ✓ Offering child pornography (soliciting others to obtain child pornography)
  - ✓ Making available child pornography (placing of child pornography online for the use of others, including by making child pornography websites)

Child pornography ("distributing...transmitting...")

- 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.

- ✓ Criminalizes:
  - ✓ Distribution of child pornography (active dissemination of child pornography)
  - ✓ Transmission of child pornography (sending child pornography through computer system)
  - ✓ Procuring child pornography for oneself or another (actively obtaining child pornography, including by downloading it)
  - ✓ Possession of child pornography (possession in computer system or data carrier)

Child pornography ("pornographic material...")

- 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.

- 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d and e, and 2, sub-paragraphs b and c.

- ✓ Governed by national standards pertaining to classification of materials as:
  - ✓ Obscene
  - ✓ Inconsistent with public morals
  - ✓ Similarly corrupt

- ✓ Materials having artistic, medical, scientific or similar merit may not be classified as pornographic

- ✓ Visual depiction includes data stored on computer system or storage medium which is capable of conversion into visual image

Child pornography ("sexually explicit conduct...")

- 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.

- 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d and e, and 2, sub-paragraphs b and c.

- ✓ Covers at least:
  - ✓ Sexual intercourse including genital-genital, oral-genital, anal-genital or oral-anal between minors, or between an adult and a minor, of the same or opposite sex
  - ✓ Bestiality
  - ✓ Masturbation
  - ✓ Sadistic or masochistic abuse in sexual conduct
  - ✓ Lascivious exhibition of genitals or pubic area of minor.
- ✓ Party may use broader definition of sexually explicit conduct
- ✓ Not relevant whether conduct is real or simulated

Child pornography ("depicts... minor...")

- 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.

- 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d and e, and 2, sub-paragraphs b and c.

- ✓ The following depictions are covered:
  - ✓ Sexual abuse of a real child
  - ✓ Images which depict a person appearing to be a minor engaged in sexually explicit conduct
  - ✓ Images, which, although "realistic", do not in fact involve a real child engaged in sexually explicit conduct; including pictures which are altered, such as morphed images of natural persons, or even if generated entirely by a computer

Child pornography ("minor…under 18 years of age")

- 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.

- 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d and e, and 2, sub-paragraphs b and c.

- ✓ Consistent with definition of child in Article 1 of the UN Convention on the Rights of the Child

- ✓ Minor generally to mean all persons under 18 years Parties may require a lower age-limit provided it is not less than 16 years

- ✓ Age refers to use of (real or fictitious) children as sexual objects; and not age of consent for sexual relations

MALABO CONVENTION: Art 29(3) (1a, 1b, 1c, 1d)) – content related offences

- **Article 29 (3) : Content related Offences**: State Parties shall take the necessary legislative and/or regulatory measures to make it a criminal offence to:

a. Produce, register, offer, manufacture, make available, disseminate and transmit an image or a representation of child pornography through a computer system

b. Procure for oneself or for another person, import or have imported, and export or have exported an image or representation of child pornography through a computer system.

c. Possess an image or representation of child pornography in a computer system or on a computer data storage medium.

d. Facilitate or provide access to images, documents, sound or representation of a pornographic nature to a minor

Poll question

You seize an audio file with the narration of a child pornography scene being played by child actors.

Is this an offence under Article 9 of the Budapest Convention?

a) Yes

b) No

Poll question

You seize an audio file with the narration of a child pornography scene being played by child actors.

a) Yes

Is this an offence under Article 9 of the Budapest Convention?

b) No

Substantive Provisions of the Budapest Convention (Part 2)

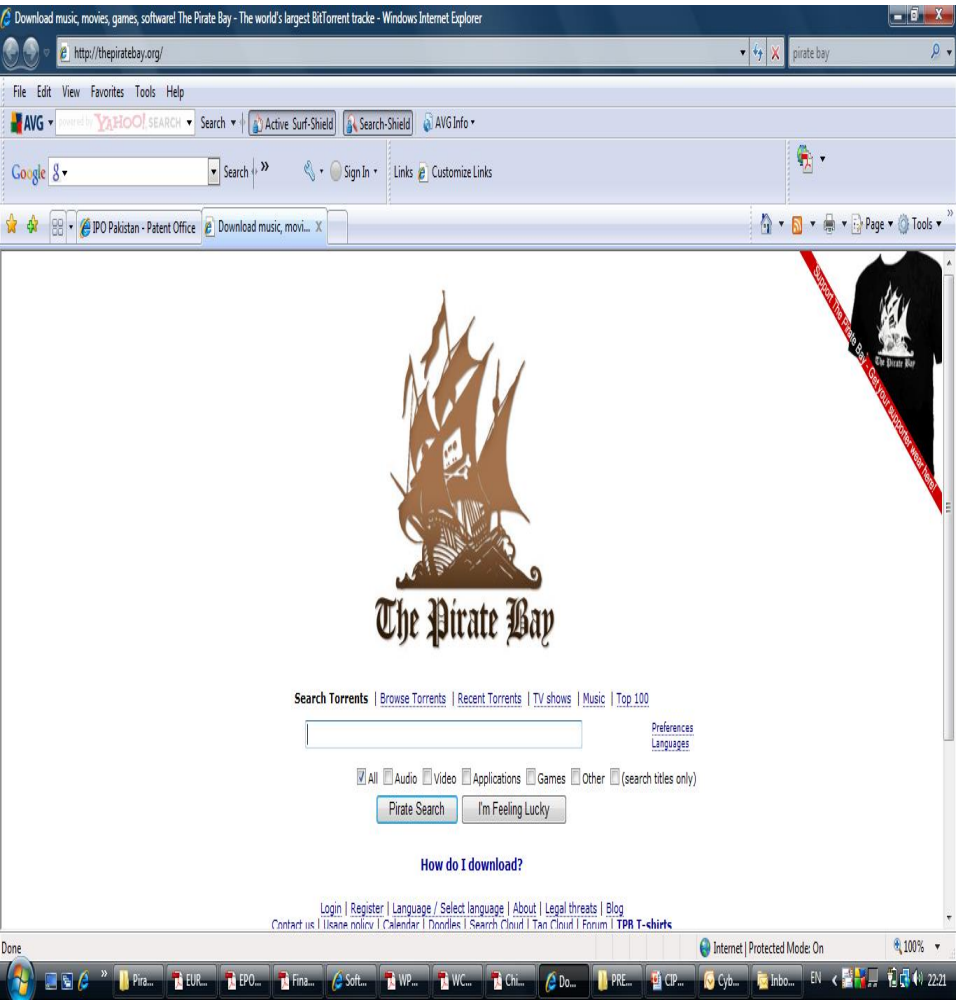
INFRINGEMENT OF COPYRIGHT AND RELATED RIGHTS

Intellectual Property Rights
(Article 10 – Budapest Convention)

- *does not create a new regulation on this subject*
- *purpose of the Budapest Convention*
  - *to apply previous rules on copyright: what is complied with the real world must be also observed within the on-line reality*
  - *infringements of copyright on-line, or committed by the means of a computer system, must be punished as if it was committed in the real world*

- Budapest Convention refers to existing international treaties
  - Paris Agreement from 24 of July of 1971
  - Bern Convention
  - WIPO treaties

Infringement of Copyright and Related Rights



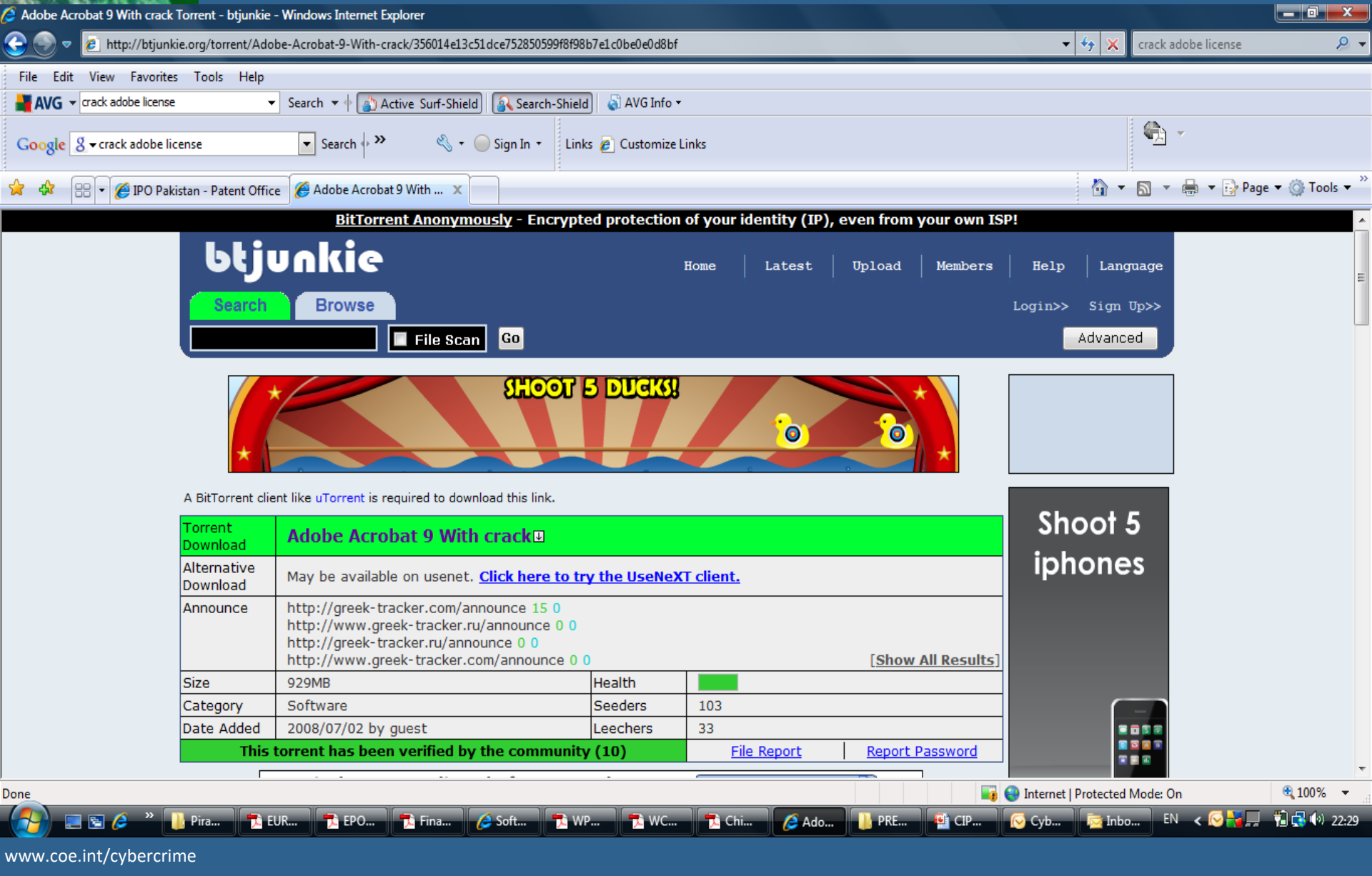
Pirate Bay co-founder arrested in Sweden to serve copyright violation sentence

By Reuters Staff

3 MIN READ

STOCKHOLM (Reuters) - One of the founders of file-sharing website Pirate Bay has been arrested in southern Sweden to serve an outstanding sentence for copyright violations after being on the run for nearly two years, Swedish police said on Saturday.

Infringement of Copyright and Related Rights



Infringement of Copyright and Related Rights ("infringement of copyright…")

- 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.**

- ✓ Criminalises wilful infringements of copyright and related rights arising from the agreements listed in the article, when such infringements have been committed by means of a computer system and on a commercial scale

- ✓ Provision merely ensures that existing copyright offences enacted pursuant to international obligations apply to acts committed through computer system

Infringement of Copyright and Related Rights ("commercial scale")

- 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 willfully, on a **commercial scale** and by means of a computer system.

- ✓ In line with Article 61 of TRIPS Agreement
- ✓ Deals with piracy on a commercial scale
- ✓ Parties may go beyond threshold of piracy on a commercial scale and criminalize other instances of copyright infringement

Infringement of Copyright and Related Rights ("infringement of related rights…")

- 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 **willfully**, on a **commercial scale** and **by means of a computer system.**

- ✓ Criminalizes willful infringements of related rights arising from the agreements listed in the article, when such infringements have been committed by means of a computer system and on a commercial scale

- ✓ Provision merely ensures that existing related rights offences enacted pursuant to international obligations apply to acts committed through computer system

Infringement of Copyright and Related Rights ("limited circumstances…")

- 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in **limited circumstances**, provided that **other effective remedies** are available and that such **reservation does not derogate from the Party's international obligations** set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

- ✓ Limited circumstances may justify not imposing criminal liability for infringement of copyright and related rights, such as:
  - ✓ Parallel imports
  - ✓ Rental rights
- ✓ However, effective remedies (e.g. civil or administrative measures) should be available in this case

Substantive Provisions of the Budapest Convention (Part 2)

ANCILLARY LIABILITY

Attempt and Aiding or Abetting ("intentionally aiding or abetting…")

- 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, aiding or abetting** the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention **with intent that such offence be committed.**

- 2 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, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c of this Convention.

- 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

- ✓ The Budapest Convention requires criminalisation of the aiding or abetting of any offence established in accordance with its provisions

- ✓ There must be intent that the offence be committed

- ✓ A service provider which provides a conduit for an offence to be committed but which does not have criminal intent cannot incur liability

Attempt and Aiding or Abetting ("attempt to commit…"

- 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, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

- 2 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, an **attempt to commit any of the offences** established in accordance with **Articles 3 through 5, 7, 8, and 9.1.a and c** of this Convention.

- 3 Each Party **may reserve the right not to apply, in whole or in part, paragraph 2** of this article.

- ✓ The Budapest Convention does not require criminalisation of attempts to all offences

- ✓ This is because it is difficult to anticipate attempts to certain offences (for instance, attempt to offer or make available child pornography)

- ✓ Attempts must be intentional to attract criminal liability

- ✓ Parties have the discretion not to criminalise attempts in whole or in part

Corporate Liability ("legal persons can be held liable…"

- 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that **legal persons can be held liable** for a criminal offence established in accordance with this Convention, **committed for their benefit by any natural person**, acting either individually or as part of an organ of the legal person, who has a **leading position** within it, based on:

  a a **power of representation** of the legal person;
  b an **authority to take decisions** on behalf of the legal person;
  c an **authority to exercise control** within the legal person.

- ✓ Four conditions need to be met for corporate liability to be attracted:
  - ✓ Commission of offence under Budapest Convention
  - ✓ Offence must have been committed for benefit of legal person
  - ✓ Person who has a "leading position" (high position in organisation) must have committed the offence
  - ✓ The leading person with the leading position must have acted on the basis of:
    - ✓ power of representation
    - ✓ authority to take decisions
    - ✓ authority to exercise control

Corporate Liability ("lack of supervision…")

- 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the **lack of supervision or control by a natural person referred to in paragraph 1** has **made possible** the **commission** of a criminal offence established in accordance with this Convention **for the benefit of that legal person by a natural person acting under its authority.**
- 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.
- 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

- ✓ Legal person can also be held liable if crime committed by someone other than leading person (for instance, employee or agent acting within scope of authority) if:
  - ✓ offence committed by such employee or agent
  - ✓ offence committed for benefit of legal person
  - ✓ commission was made possible due to leading person having failed to take reasonable or appropriate measures to supervise the employee or agent
- ✓ Does not mandate general surveillance over employee communications

MALABO CONVENTION: Art 30(2) – criminal liability for legal persons

State Parties shall take the necessary legislative measures to ensure that legal persons other than the State, local communities and public institutions can be held responsible for the offences provided for by this convention, committed on their behalf by their organs or representatives. The ability of legal persons does not exclude that of the natural persons who are the perpetrators of or accomplices in the same offences.

Session objectives

By the end of the session, delegates will be able to:

- Identify the elements which constitute the offence of:
  - Computer-related forgery
  - Computer-related fraud
  - Child pornography
  - Infringement of copyright and related rights
- Understand how the Budapest Convention criminalises aiding, abetting and attempting offences, and the scope of corporate liability

Introductory Judicial Training Course on Cybercrime and Electronic Evidence

Thank you

Xxxxx XXXXXXXX

Council of Europe

email

DD Month YYYY