INTERNATIONAL LAW IN INFORMATION TECHNOLOGY

By Group Captain P Aanand Naidu (retd)

What is Cyber Law

Cyber Law is the law governing cyber space. Cyber space is a very wide term and includes computers, networks, software, data storage devices (such as hard disks, USB disks etc), the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc.

Rules of Conduct

Law encompasses the rules of conduct

- that have been approved by the government, and
- which are in force over a certain territory, and
- which must be obeyed by all persons on that territory.
- Violation of these rules could lead to government action such as imprisonment or fine or an order to pay compensation.

What does it encompass

Laws include

- Cyber Crimes
- Electronic and Digital Signatures
- Intellectual Property
- Data Protection and Privacy

What does it encompass

Laws include

- Copyright law in relation to computer software, computer source code, websites, cell phone content etc, • software and source code licences
- Trademark law with relation to domain names, meta tags, mirroring, framing, linking etc
- Semiconductor law which relates to the protection of semiconductor integrated circuits design and layouts,
- Patent law in relation to computer hardware and software

Uniqueness of Cyber Crimes

- Intangible
- Disrespect for jurisdictional boundaries.
- Traffic volumes
- Open to participation by all
- Anonymity –citizens
- Economic efficiency
- Extreme mobility and Speed

Legislation

Due to single technical standards Internet services are globally available

Unlike the technical standardisation the legal frameworks that address Cybercrime can differ significantly

Legislation....

Legislation plays an important role, including as part of prevention strategies

States will refer to means of criminal law to enable investigation of acts of cybercrime

Without adequate criminalization, law enforcement agencies will not be able to carry out investigations and identify those who put security at risk

Legal Framework

International Agreements

Bilateral Agreements

National law

Internal regulations

Evolution of International Law

Cyber Security is an emerging **area of law**

International Cooperation essential

The international **level of consensus** on criminal law has not been achieved.

International Bodies / UN

GA Resolutions

Developments in the Field of Information and Telecommunications in the Context of International Security

Combating the Criminal Misuse of Information Technology

Creation of a Global Culture of Cybersecurity

Creation of Culture and the Protection of Critical Information Infrastructures.

International Bodies

ITU - Global Cybersecurity Agenda (GCA)

INTERPOL - Coordinating law-enforcement agencies and legislations

NATO - Cyber Defense Policy and Concept

G8 High Tech Group - Recommendations and Best Practices

OECD, several regional organizations

Cooperation and Law

- Bilateral/multi-lateral agreements provide legal basis for mutual cooperation (investigation, prosecution, extradition etc.)
- Countries with no legal coverage in the field are a good “jurisdiction shopping forum”
- nternational discussions do not stand in court, different arguments and legal schools need to be balanced
- Law is important, but secondary means in ensuring effective cyber security

European Council

- **Convention on Cybercrime (C^3)**
- Opened for signatures **2001**
- Entry into force 2004
- **Open to MS and non-MS**
- **46 member states**

Criticism

- **Soft law or insufficient number of states parties**
- Different views as to whether there are gaps in international law in general
- Difficult to achieve additional consensus
- Focus to be put on ensuring the effective implementation of the conventions

European Union

Directives:

- Personal Data Protection
- Data Retention
- Electronic Communications
- ISP liability
- Information Society Services
- Spam
- Critical Infrastructure Protection

Estonian Lessons

- Adding the critical infrastructure protection context to computer-related crime provisions of the Penal Code
- Criminalizing preparation of computer-related crime
- Viewing computer-related crime as terrorist crime
- Defining critical information infrastructure
- More specific regulation on ISP liability

Budapest Convention: 2001

- The only convention
- **Reforms long overdue**
- **No binding international convention**
- **Disharmony is the cause**

Budapest Convention: 2001

- The Convention provides for four broad categories of substantive offence
- Offences against the confidentiality, integrity and availability of computer data and systems
- Computer-related offences (computer-related fraud and forgery)
- Content-related offences (child pornography)
- Criminal copyright infringement.

Crime Congress: Bangkok(2005

- Within the preparatory meetings, several Member States called for an UN Convention on Cybercrime
- Topic was discussed during the Congress
- Member states decided not to initiate such a process

Crime Congress: Salvador 2010

- All four regional preparatory meetings called for the development of an international instrument on Cybercrime
- Member States decided to strengthen capacity building and to undertake a comprehensive study of the problem of cybercrime and responses to it

Introduction to Privacy

- Definition

  "the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others

- Dimensions of privacy:

  1) Personal privacy

  Protecting a person against undue interference (such as physical searches) and information that violates his/her moral sense

  2) Territorial privacy

  Protecting a physical area surrounding a person that may not be violated without the acquiescence of the person

  3) Informational privacy

  Deals with the gathering, compilation and selective dissemination of information

Basic Principles

Basic privacy principles

- Lawfulness and fairness
- Necessity of data collection and processing
- Purpose specification and purpose binding
  - There are no "non-sensitive" data
- Transparency
  - Data subject´s right to information correction, erasure or blocking of incorrect/ illegally stored data
- Supervision (= control by independent data protection authority) & sanctions
- Adequate organizational and technical safeguards

Privacy protection can be undertaken by:

- Privacy and data protection laws promoted by government
- Self-regulation for fair information practices
- Privacy-enhancing technologies (PETs) adopted by individuals
- Privacy education of consumers and IT professionals

Threats to Privacy

Threats to privacy at application level

- Threats to collection / transmission of large quantities of personal data
- Threats to privacy at communication level
- Threats to privacy at system level
- Threats to privacy in audit trails

Threat to Privacy

- Identity theft – the most serious crime against privacy

- Threats to privacy – another view
  - Aggregation and data mining
  - Poor system security
  - Government threats
    - Gov't has a lot of people's most private data
      - Taxes / homeland security / etc.
    - People's privacy vs. homeland security concerns
  - The Internet as privacy threat
    - Unencrypted e-mail / web surfing / attacks
  - Corporate rights and private business
    - Companies may collect data that U.S. gov't is *not* allowed to
  - Privacy for sale - many traps
    - "Free" is not free…

Privacy Controls

Technoical Controls

Legal Controls

Comrehensive Laws

Sectoral Laws

A Common Approach: Privacy Impact Assessments

* An evaluation conducted to assess how the adoption of new information policies, the procurement of new computer systems, or the initiation of new data collection programs will affect individual privacy
* The premise: Early stages intervention will reduce potential adverse impacts

A Common Approach: Privacy Impact Assessments

- Requirements:
  - PIA process should be independent
  - PIA performed by an independent entity (office and/or commissioner) not linked to the project under review
  - Participating countries: US, EU, Canada, etc.

Legal Privacy Controls : A Common Approach:

* EU implemented PIAs
* Under the *European Union Data Protection Directive*, all EU members must have an independent privacy enforcement body
* US passed the E-Government Act of 2002 which requires federal agencies to conduct privacy impact assessments before developing or procuring information technology

Information Sharing-CERT

* Information sharing and Joint Response
  * CERT to CERT communications
  * Cybercrime 24/7 Network (G-8)
  * APCERT (Aust/Japan/South Korea etc)
* Standards
* Laws

Org for Econ Coop Dev

* Working to promote the ‘Culture of Security’ Guidelines with other economies
* Encouraging OECD economies to sponsor projects to strengthen e-security of developing economies in their regions.

FUTURE

* Because of the borderless nature of cyberspace, international cooperation is even more essential to secure a safe online environment.
* More businesses and governments and business machinery online
* A ‘target rich environment’

FUTURE...

Governments and business who are the major users of the internet will be forced to work together to combat the worst elements

Technology will provide some help – eventually

THANK YOU