Essentials of Law

**Internet Law in respect to the IT Law**

|  |  |
| --- | --- |
| Name | Registration number |
| Ariyasinghe H.L.P | 154005A |
| Weerasingha N.M. | 154130C |
| Rajapaksha R.P.M.P. | 154090C |
| Wikramasinghe Y.L. | 154137E |
| Rathnayake C.J. | 154143J |

Date of submission: 24th November 2017

**Chapter 1**

**Introduction**

In this report we wish to discuss about the Internet law took place relating to the IT law. Here we go through this topic as what is IT law ,what is Internet law, Evolution of Internet law, present legislations of IT law related to the Internet law, Importance of IT law, Actions get when break Internet law.

In first chapter we wished to give some kind of brief knowledge about IT law .In the next chapter we discussed what is Internet law. In the third chapter we discussed Evolution of Internet law in descriptive manner. In the fourth chapter we focused on the present legislations of IT law related to the Internet law. In the last chapter we discussed what are the actions that are taking place when breaking Internet law.

Nowadays Information Technology is take a place as a rapidly and continuously developing section. The society building networks through the IT to the convenience of their information's handling. Internet is the main component where people build these interconnection with peoples and information. So accordingly with this development of internet with respect to the IT, the number of crimes also increased. As a result different parts also added to the law with the time. This was took place in the evolution of law related to the IT law.

**Chapter 2**

**2.1 What is IT law ?**

Information Technology Law (also referred as Cyber Law) is a set of recent legal legislation, currently in existence in several countries, which judge the process and actions of information handling. These legal enactments cover a broad area of different aspects relating to computer software, protection of computer software, access and control of digital information, privacy, security, internet access and usage, and electronic commerce.

In Sri Lanka the IT Law is intended to create the enabling legal environment for the development of Information and Communication Technology(ICT), through the enactment of the required laws by Parliament in order to facilitate e-Government, e-Business as well as to attract ICT related foreign direct investment. The Sri Lankan computer crime Act No.24 of 2007 primarily address computer related crimes and hacking offences. Content related offences are being addressed through a series of changes to the Panel Code and other statutory provisions. There has been an increasing of cybercrime complains within the last few years according to the Sri Lanka, Computer Emergency Response Team (SLCERT).

Traditional crime has long ago moved online. Crimes like money laundering, child pornography, sexual exploitation of children, sale and trafficking of illegal drugs, prostitution, internet fraud, credit card fraud, illegal gambling, hate propaganda, racism crimes, intellectual property theft, piracy harassment, stalking threats, extortion identity theft and many more.

**2.2 What is Internet Law**

Internet law is about the legal issues, legal principles and legislation for the use of internet. Another term for internet law is cyber law. Especially internet law cannot be identified as a solid field, actually it incorporates and uses in several fields such as privacy law or contract law. The laws which govern internet will require a unique structure to attach with the international and ethereal nature of the web. Many argue the Internet is not actually “regulable” at all, while others argue that not only can it be regulated but substantial bodies of law already exist. Because of the Internet is not geographically bound, national laws can not apply globally for the internet issues. Some believe that the internet should be operated as if it were a land all its own, independent of national policy. Internet Law is a special case because, given the breadth and complexity of the internet and all of its potential liabilities, internet laws must be flexible enough to cover countless real and theoretical possibilities. Further internet law can be included the following areas.

* Laws related to creation of websites.
* Laws governing ISP(Internet Service Provider)
* Laws related to how trademarks are used online
* Laws regarding how to resolve conflicts over domain names
* Laws related to how to link web pages

In countries such as China, Saudi Arabia, and Iran, the internet is greatly censored. This censorship aside, there are generally four ways the internet is overseen. The four methods include Laws, architecture, Norms and markets.

Other topics that have been affected by the rise of the Internet, include areas such as privacy, intelligence gathering, fraud, cyberbullying, and cyberterrorism. As quickly as technology evolves, so too will the various legal issues presented by these innovations.

**2.3 Evolution of Internet Law in respect to IT Law**

1. **The Birth of the Non-Commercial Internet**

In 1974, Vent Cerf and Bob Kahn was designed the “Transmission Control Program/Protocol” (TCP).This helps computers to connect with each other. In 1976, Bill Gates and Paul Allen were founded the Microsoft. In 1978 First spam email was transmitted. The internet has not any law or any rule prior to the mid-1990s.

1. **The Birth of the Commercialized World Wide Web**

In the mid-1990s World Wide Web (WWW) was developed and early years domain name registered was done free of charge. But in 1995, NSF started to charge $50 annually for registration. This caused to commercialization of Internet. With the increase of the internet usage, it’s began to conflicting with legal disputes.

**C. The Commercialized Internet**

In 1994, Pizza Hut started to take online orders through the internet. The first Internet gambling casinos were started in 1995. Then Internet law was organized when thousands American went online. This commercialization caused to create new rules for internet such as copyrights, for domain names, Trademarks…etc. When businesses firms started to sell services and products through the internet courts also began to resolve Internet- related jurisdictional.

1. **Google-ization**

Google was named as the most popular search engine in1985.More features were added (google search, google groups, Google toolbar, Google print, Google eBook, and Google map) day by day and multi-language (26 different languages) availability came in 2001. With this newly added features caused to add some rules and regulations to the current law.

**E. Walled Gardens, Social Networks & Other Developments**

Fifteen years ago google was created the “walled gardens” like “Apple’s mobile devices” and “Google’s suite) .In 2001 Wikipedia was founded. Ability of sharing personal interesting’s through YouTube, Facebook, Second life,Tweeter,Flicker was began from 2005 and it is grownup anew IP issue about the copyright ability of tweets. So it was limited to maximum size of a tweeter message to 140 characters. In china rapidly increased the internet users up to 22 million in 2000 to 2004.So the Internet law is rapidly evolved as international, Government, trade, courts decisions. This evolution created the “legal lag” problem.

**2.4 A brief history of legal lag**

Court and legislatures have add new rules and laws when the Internet creating more facilities and features. In 2010 law dispute was arising against the CEO and the Facebook founder “Mark Zuckerberg”, for stolen the ideas of Harvard classmates to develop his applications. There was an issue of Facebook posting and a ninth grade school children was filed a sex discrimination case. The third circuit observed and found how FB and other “stream-of-consciousness communications” and they were rearranged the first Amendment.

**How Personal Jurisdiction Has Adapted to the Internet**

Internet is a networking among whole world and it is created unique rules as technology not respect to the national borders. Most of them are for domain names and domain name activities. There is no international convention that addresses Internet. New Internet cases and developments are being decided on a daily basis.

**Internet Law Timeline**

The first court decision regarding the internet was taken in 1991.In this era computer hacking cases also began. A computer hacker was convicted for gaining unauthorized access to BellSouth’s 911 computer files and publishing this proprietary information in a hackers’ newsletter. In 1995, Senator J. James Exon of Nebraska introduced the Communications Decency Act (CDA).

**How the Internet Shaped IP Law**

IP rights based on, how branches of IP addresses accommodated the WWW. Judge Easterbrook was revealed that the internet has some liabilities and IP rights.

**Copyrights in Cyberspace**

Courts published copyright law in a “series of cases and statutes that enshrine the idea of property interests in cyberspace”. In 1996, more countries and organizations were entered to this law. (EX: World Intellectual Property Organization (WIPO) Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT).)

**2.5 Present legislations of Internet Law with respect to IT law.**

Information and communication Technology is a very important and developing section in the Sri Lanka. As well as technical and economic environment has been developed with the use of technology I this situation. By today Information Technology acts a major role, therefore it is important to provide the necessary legal environment for using electronic devices and services for official as well as personal purposes. Further, the activities which are affected to IT should be controlled by the different kinds of acts and regulations.

* Information and Communication Technology Act No.27 of 2003,
* Evidence (Special Provisions) Act No.14 of 1995 ,
* Intellectual Property Act No. 36 of 2003 (Sections related to Copyright),
* Electronic Transactions Act No. 19 of 2006 ,
* Computer Crimes Act No. 24 of 2007 ,
* Payment And Settlement Systems Act, No. 28 of 2005 ,
* Payment Devices Frauds Act No.30 of 2006, are acts related to internet law in respect to IT law.

**Information and Communication Technology Act No.27 of 2003**

This is an act which provides implementation of strategies and programs for Information and Communication Technology in Sri Lanka. CINTEC (Computer and Information Technology Council of Sri Lanka) established the committee on law and computers.

**Evidence (Special Provisions) Act No.14 of 1995**

An act to provide for the admissibility of audio visual recordings, and of information contained in statements produced by computers in civil and criminal, proceedings.

**Intellectual Property Act No. 36 of 2003 (Sections related to Copyright)**

An act to provide for the law relating to intellectual property and for an efficient procedure for the registration, control and administration there of ; to amend the customs ordinance (chapter 235) and the high court of the provinces (special) provisions act, no. 10 of 1996 ; and to provide for matters connected therewith or incidental thereto

**Electronic Transactions Act No. 19 of 2006**

This is the Act which is facilitating e-commerce, e-Signature-e-Contracting and electronic transactions on Law of IT.

**Computer Crimes Act No. 24 of 2007**

In last few years there are several modifications applied to the act and it has been enacted as the Computer Crimes Act No.24 of 2007.The Act has been introduced provisions for criminal implications regarding unauthorized access to a Computer, Computer Programs and unauthorized use of a Computer.

**Payment and Settlement Systems Act, No. 28 of 2005**

This Act may be cited as the Payment and Settlement Systems Act, No. 28 of 2005 and shall come into operation on such date as the Minister may by Order published in the Gazette appoint.

**Payment Devices Frauds Act No.30 of 2006**

This is an act, giving power to prevent the possession and use of unauthorized payment devices such as deals with credit card frauds.

**2.6 Advantages of Internet law**



* To ensure the enforcement and protection of intellectual property, trademark and copyrights.
* Nowadays most of the people work with the technology and Internet (emails, mobile phones…etc.). Even in Non-cybercrime cases evidence may be found in computers. So cyber law is most important thing.
* Child online Protection Act of 1998 (Title 47 U.S.C. Section 231) Makes it a crime for site operations to fail to use proper technology and methodology to prevent minors from accessing “harmful” materials.
* Lankham Act of 1976 (Title 15 U.S.C. 1051) – Provide the protection of trademark and copyrights.
* Trademark Dilution Act of 1996 (Title 15 U.S.C. section 1125) – Ensure the protection of holders of computer related trademarks from the effect of domain-page registrations.
* The Communications Decency Act of 1996 (CDA) (Title 47 U.S.C. SECTION 223) – gives the protection from defamation suits to internet service providers.
* IT Act 2000 – Any company can store data as electronically. This gives the protection to the data
* Reduce computer crimes and ensure the privacy of Internet users.

**2.7 Cyber Crimes/Internet Crimes**

There are three major categories of cyber crimes

1. Internet Crime against persons

This happens against persons through the computer or the internet .This includes cyber harassment, transmission of child – pornography, cyber stalking, sms problems, credit cards frauds, cracking…etc.

1. Internet-crimes against Property

This includes Worm attacks, IPR violations, Cyber-squatting, hacking, intellectual property theft, Virus transitions etc.

1. Internet Crimes against government

Mostly this consists hacking into confidential government data, cyber warfare, cyber terrorism etc.

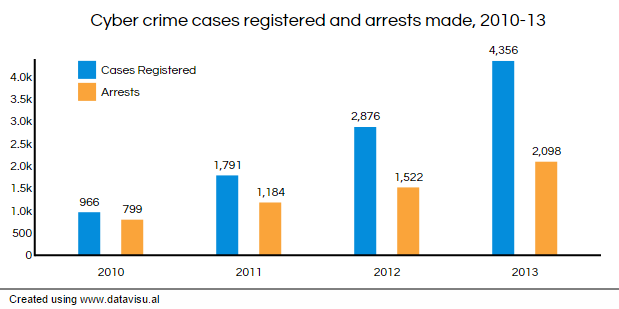


Figure 2.1 cyber-crime cases graph

**2.8 Actions that are taking place when breaking Internet Law**



There is a variety of issues arise in considering the application of the criminal law to instances of computer – related conduct. One of the most critical is whether computer - related conduct should be regarded as requiring technology – specific legislation or whether it might satisfactorily be regulated through the application of more general criminal law provisions. Although a trend can be identified throughout Europe and the US to enact computer crime statutes, experience in the UK with the Computer Misuse Act 1990 suggests that such an approach is not without its pitfalls. The debate preceding the enactment of this statute was notable for a difference of opinion between the law commissions for Scotland and England concerning the scope of such legislation, the Scottish Law Commission being considerably more sanguine about the effectiveness of general provisions of the criminal law.

Another issue which is sometimes neglected in the debate on the role of the criminal law concerns the availability of other legal remedies.

The relevance of alternatives sanctions in considering whether an extension of criminal law is warranted was accepted in Home Office Guidelines, published in 1982, outlining principles to be taken into account in determining whether new criminal provisions should be introduced. First, it was stated, the behavior must be so serious that it cannot satisfactorily be dealt with on the basis of civil law remedies, damages. Second, criminal sanctions should only be created where other less drastic means of control would be ineffective, impractical or insufficient. A final principle required that any new offence should be susceptible to enforcement.

The Act is cited as the Computer Crime Act, No.24 of 2007.

* If any computer or information is accessed intentionally by a person to secure himself or someone else the following actions will take place.

1. Will be charged a fine not exceeding one hundred thousand rupees, or to imprisonment of less than 5 years, or both fine and imprisonment.
2. Will be charged a fine not exceeding two hundred thousand rupees, or to imprisonment which extends 5 years, or both fine and imprisonment.

* If any computer or information is accessed intentionally by a person knowing the result is a danger to national security, the national economy or public order the following actions will take place.

1. Will be punished with an imprisonment of less than 5 years.

* If any subscriber information or traffic data or any communication, to, from or within a computer or any electromagnetic emissions from a computer that carries any information is accessed intentionally by a person

Will be charged a fine more than one hundred thousand rupees and not exceeding three hundred thousand rupees, or to an imprisonment of not less than six months and not exceeding three years, or both fine and imprisonment.

* If a computer or a computer program, a password or similar information by which the whole or any part of a computer is capable of being accessed is accessed intentionally by a person

Will be charged a fine more than one hundred thousand rupees and not exceeding three hundred thousand rupees, or to an imprisonment of not less than six months and not exceeding three years, or both fine and imprisonment.

* Any person who, being entrusted with information which enables him to access any service provided by means of a computer, discloses such information without any express authority to do so or in breach of any contract expressed or implied

will be charged a fine not less than one hundred thousand rupees and not exceeding three hundred thousand rupees or to an imprisonment of either not less than six months and not exceeding three years or to both such fine and imprisonment.

* If someone abets the commission of an offence under this Act shall be guilty

1. if the offence abetted is committed in consequence of the abetment, be liable to the same punishment as is provided for the offence.

(b) if the offence is not committed in consequence of the abetment, be liable

(i) where the maximum fine or term of imprisonment is provided for, to a fine not exceeding one fourth of the maximum fine provided for the offence or to imprisonment of either description for a term not exceeding one fourth of the maximum term provided for the offence, or to both such fine and imprisonment.

(ii) where the maximum fine or imprisonment is not provided for or the maximum term of imprisonment is life, to a fine not exceeding two hundred and fifty thousand rupees or to imprisonment of either description for a term not exceeding five years, or to both such fine and imprisonment.

* Where an expert or a police officer is satisfied that any information stored in a computer is reasonably required for the purposes of an investigation under this Act and that there is a risk that such information may be lost, destroyed, modified or rendered inaccessible, he may by written notice require the person in control of such computer or computer system to ensure that the information be preserved for such period not exceeding seven days as may be specified in such notice.
* On an application made to a Magistrate having jurisdiction, the period for which the information is to be preserved may be extended for such further period, which in the aggregate shall not exceed up to ninety days.
* The actions taken for Facebook crimes are as follows.

1. For the mental damages shall be guilty of an offence and shall on conviction be liable both to a fine of one fifty thousand rupees and to imprisonment of either description for a term two years.
2. For hacking Facebook accounts shall be guilty of an offence to imprisonment of either description for a term two years.
3. For keeping fake Facebook accounts with unnecessary videos/photos shall be guilty of an offence to imprisonment.
4. For helping and encouraging another person or people to do such things will also be guilty of an offence to imprisonment.

* For the purpose of an investigation under this Act, an expert called upon to assist any police officer shall, have the power to—

(a) enter upon any premises along with a police officer not below the rank of a sub-inspector ;

(b) access any information system, computer or computer system or any programme, data or information held in such computer to perform any function or to do any such other thing

(c) require any person to disclose any traffic data

(d) orally examine any person

(e) do such other things as may be reasonably required, for the purposes of this Act.

**Chapter 3**

**3.1 Conclusion**

Here we have discussed about the IT law which is a part of the internet law. Internet law which is also known as Cyber law is about the legal issues, legal principles and legislation for the use of internet. Laws, architecture, Norms and markets are the four ways the internet is overseen.

Evolution of internet law describes the way the factors have been extended.

Cybercrimes take place against persons, property and government. We have to take actions in controlling the cybercrimes such as,

* Computer –related fraud
* Computer forgery
* Damage to computer data or programs
* Unauthorized access
* Unauthorized interception
* Unauthorized reproduction of a protected computer program
* Alteration of computer data or computer program
* Computer espionage
* Unauthorized use of a computer
* Unauthorized use of a protected computer program etc

So to protect our data from unauthorized accesses, we must agree with the Ministry of Justice that the Act has contributed to a culture of greater openness across public authorities, particularly at central Government level which was previously highly secretive. There are many advantages of the internet law.

We must welcome the efforts made by many public officials not only to implement the Act but to work with the spirit of FOI to achieve greater openness. Our report shows that the strength of the new culture of openness is, however, variable and depends on both the type of organization and the approach to freedom of information of the individual public authority.

**Chapter 4**

**References**

* <http://www.cbsl.gov.lk>
* <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.462.3873&rep=rep1&type=pdf>
* <http://www.commonlii.org>
* <https://expertcyberlawyer.com/meaning-of-cyber-law-and-importance-of-cyber-law>
* <https://www.hg.org>