Protecting Personal Information in the Era of Cyber Crime

DISSERTATION SUBMITTED TO DAFFODIL INTERNATIONAL UNIVERSITY
IN PARTIAL FULLFILMENT OF THE REQUIREMENT
FOR THE AWARD OF THE DEGREE OF

MASTERS OF LAWS

2018

Md. MozammelHoque

Id: 181-38-244

FACULTY OF HUMANITIES AND SOCIAL SCIENCE
DAFFODIL INTERNATIONAL UNIVERSITY
DHAKA 1207
2018
"© Daffodil International University"

Dedicated to my Family

"© Daffodil International University"

Declaration and Certificated

Date: 23-12-2018

Declaration

I absolutely aware that I actually have associate degree obligation to create clear to the administrative official that is my very own work, and that is that the work of others whom I'm citing in my paper. Unless, I clearly indicate otherwise, my administrative official is entitled to assume that everything being conferred within the paper originates from Pine Tree State. I conjointly declare that I actually have not submitted this paper or any a part of it, for assessment in any of my graduate work or different educational endeavors. I conjointly absolutely aware that restoring to plagiarism would lead Pine Tree State to get a mark of 'zero' and expose United States to additional disciplinary actions as prescribed by the University's rules and rules.

Md. MozammelHoque
LL.M.
ID: 181-38-244
Department of Law
Daffodil International University

"© Daffodil International University"

CERTIFICATE

This is to certify that the thesis on "**Protecting Personal Information in the Era of Cyber Crime**" is done by **Md. MozammelHoque** in the partial fulfillment of the requirement for the degree of LL.M. from Daffodil International University of Bangladesh. The thesis has been carried out under my guidance and is a record of research which carried out successfully.

Mr. Md. Riaduzzaman
Head
Department of Law
Daffodil International University

Md. Abu Saleh
(Advisor)
Senior Lecturer
Department of Law
Daffodil International University

"© Daffodil International University"

Acknowledgment

At first, I would like to thanks our merciful and the most passionate ALLAH for giving us the opportunity to complete our dissertation. The purpose of this dissertation is to present my topic as clearly as possible, as briefly as practicable.

I have completed my dissertation on Protecting Personal Information: Should it be legalized in Bangladesh?"

This dissertation represents the details of the basic concepts like definition, classification, characteristics, history, legal documents with some case references etc. On Protecting Personal Information.

Unavoidably, there may occur some mistakes in this dissertation but we have tried with my maximum effort to include correct and important data.

So, I request please avoid the mistakes and consider the only positive sides of this dissertation.

"© Daffodil International University"

List of Abbreviation

ACLU American Civil Liberties Union

ASEAN Association of Southeast Asian Nations

ATM Automated Teller Machine

CERT Computer Emergency Response Team

CA Cyber Attack

CC Cyber Crime

DOD Department of Defense

DOJ Department of Justice

EC European Community

FAA Federal Aviation Administration

FATF Financial Action Task Force

FBI Federal Bureau of Investigation

FTC Federal Trade Commission (U.S.)

ICC International Chamber of Commerce

ICJ International Court of Justice

IMO International Maritime Organization

IO Information Operations

IT Information Technology

ITU International Telecommunication Union

MCCD Multi-Community Cyber Defense

"© Daffodil International University"

MLAT Mutual Legal Assistance Treaty

NASA National Aeronautics and Space Administration (U.S.)

NATO North Atlantic Treaty Organization

OAS Organization of American States

OECD Organization for Economic Cooperation and Development

PRB People's Republic of Bangladesh

RFC Request for Comments

SARPs Standards and recommended practices

SCADA Supervisory Control and Data Acquisition

TCP Transmission Control Protocol

UN United Nations

UNDP United Nations Development Program

U.K. United Kingdom

U.S. United States

"© Daffodil International University"

Table of Contents

"© Daffodil International University"

"© Daffodil International University"

"© Daffodil International University"

Chapter 1

INTRODUCTORY CHAPTER

1.1 Introduction:

The Internet has bring in instantaneous and inexpensive announcement from corner to corner the earth and its remodel business by create it easier for public to work together from corner to corner an untidiness of jurisdiction[1]. On the other hand the opening of the network has bring with it consequential risk and danger and it's be converted into at risk to cyber-attacks[2]. Refined against the law network are maltreatment Net to hand over new against the law behaviors in opposition to easy to fool and susceptible pc users United Nations organization use the web to carry out their on a daily basis behavior, like cause e-mail in receipt of products and conversation on communal network site. The rapidity of the network conjointly to challenges the supremacy of lawmakers to supervise it in point of fact. The insignificance of the network has conjointly expedite cyber offence like deception this happen once a human being individual information in the vein of bracket together in treatment individuality file is with authorization obtain and thenceforth wont to hand over robbery or deception. Will be dedicated at the same time as not technological means that via bodily or very old earnings that or by junk mail robbery or on-line[3].

The individuality against the law uses the data inhume alia to unlock credit of the financial records, unlock store financial records, buy goods and stand up amount outstanding amounting to a range of rand surrounded by the wounded' name. Therefore, individual information is unacceptably obtain by deception, and in addition the individuality thief use the identity-connected information or awareness to commend illegal behavior surrounded by the wounded names. The cyber attack disturbed activate in an exceptionally multi-jurisdictional ambiance, that made the next and hearing of such offender difficult and problematical. Deception is supposed by a number of to be

[1] Fawzia Cassim. BA (UDW) LLB (UN) LLM LLD (UNISA).

[2] Nuth, 2008 CLSR 437-438; Rubin 1995(IJLFT) 118; Goodman and Brenner 2002 IJLIT 144, 160.

[3] Information and Commission Technology Act, 2006

a fresh enlargement. In spite of this, it's approved that the impression and use wrongly of identity credentials have exist for to a certain extent it deliberate. As an instance this, the misuse of identity-related info was according throughout the Nineteen Eighties[4]. Identity thieves have used alternative ways like choose shoplifting and thieving identity-connected information from mailboxes to get and use wrongly nation's credit and classification credentials.[5] The coming out of knowledge and also the digital era is suspected to have power over made to order the target and conduct of such offender. Without a doubt, the pace of scientific improvement and also the exaggerated use of information skill have provide identity thief with original, supplementary with good grace-obtainable source of confidential information. Fraud possibly will be a commit a breach of safety measures that is significant to the network and e-exchange communication[6]. It undermine e-commerce communication. A get higher surrounded by the use of most recent phone call technology has so see a follow-on add to surrounded by the charge of deception as vulnerabilities in pc network are open to the elements and out of order. Fraud disrupt the live of thousands of persons each year.

As such, crime is also one in every of future massive problems governments can face within the medium to short term. Given the borderless nature of crime, it's fascinating, of course, that they determined to face it along which selections be crazy a solid data of all the challenges concerned. As this paper can conceive to demonstrate, such challenges are broad and complicated and canopy technical, territorial and moral aspects. Some overlap across these 3 aspects and a few interleave[7].

1.2 Background:

The primary record cyber crime accepted surrounded by the year 1820! that's not appalling taking into consideration the definite information that the abacus, that is unspecified to be the initial assortment of a pc, has been in the region of since 3500 B.C. in India, Japan, and China. The time

[4] http:www.itu.int ITU cyber security/ legislation/ html>

[5] ibid 25

[6] ibid 26

[7] ibid 26

"© Daffodil International University"

of current computer, on the other hand, begin with the logical steam engine of Charles Babbage.[8] In 1820, Joseph-Marie Jacquard, a textile producer in France, produced the become visible. This piece of equipment allowable the reduction of a sequence of ladder surrounded by the weave of out of the ordinary equipment. This resulted in a exceptionally be concerned in the midst of Jacquard's human resources that their very old employ and hold up were human being susceptible. They dedicated acts of interfere with to dishearten Jacquard category any use of the new equipment. This can be the most important record law-infringement. These days computer have come back and comprehensive means, with neural network and nano-compute shows potential to give you an idea about every one tiny part in a exceptionally goblet of hose down into a pc competent of performing arts Billion operation per moment.

Cybercrime is a wickedness have its starting point contained by the on the increase confidence on computer in up-to-the-minute life. in a very day-age once the whole thing from microwave ovens and refrigerators to insignificant get-up-and-go scrub is life form run on computer, law-contravention has suspect rather threatening implication. Main cyber crime contained by the fresh what went before clinch the Citibank chisel. $10 million were deceptively transfer out of the bank and into a examination relation in Swiss confederacy. A Russian hacker come together LED Vladimir Kevin, a distinguished hacker, perpetrate the do violence to. The come together compromise the bank safety measures system. Vladimir was purportedly exploitation his place of work pc at AO Saturn, a pc firm in St. Petersburg, Russia, to break off into Citibank pc. He was at last stationary at Heathrow on the wing sports ground on his credit to Switzerland Confederation.[9]

1.3 Literature Review:

The term cyber-crime has been a serious topic deliberate by a lot of folks by means of totally dissimilar views on the topic, a bigger share upcoming back at it starting a special perspective than the others. Cyber-crimes have superior on top of conventional crime and at present have discouraging penalty to the countrywide safekeeping of scientifically residential country. Cyber

[8] Lane and Sui 2010 GeoJournal 46

[9] file:///E:/New%20Folder%20(2)/THISIS/Downloads/Documents/introduction.pdf, Last visited 30 June 2010].

"© Daffodil International University"

attacks in opposition to cash armed forces establishment have be converted into supplementary recurrent, supplementary experienced, and extra prevalent. Though small-level rejection-of-examination attack adjacent to most important currency establishment produce the primary headline, group of people and provincial bank, credit unions, money transmitters, and third-party repair suppliers have experienced try breach in latest years.

Including the document that affirm that "the adoption by all countries of applicable legislation against the misuse of data and Communication Technology (ICT), for criminal or alternative functions, together with activities supposed to have an effect on the integrity of national crucial data infrastructures, is central to achieving world cyber security".

The unlawful deed is also directed at a computer's set of connections or diplomacy e.g., CPU curriculum, denial of service attacks (DOS), malware. The forbidden legal document is also assist by a set of connections or policy with intention self-employed of the pc set of connections or device". associate cyber-crime to the forces in an extraordinarily document representation his unqualified attention contained by the country's armed well-being, Major General Umo outline that crime, cyber rebel act, cyber conflict, cyber safety measures four-sided figure determine one and as a result the similar issue. Reason being, theft or fake heading for at an important person or a business is corresponding to hostility the hostilities on the objective of the offense. Exertion to undertake network offense hold in your weapons proceedings connected to defensive network.

Some instances of cyber crimes includes causing spam e-mail burglary individual information infringement into somebody's laptop to look at or alter information (hacking) and trick an important person into informative their individual information (phishing), create network armed forces out of stock for users (Denial of service –DOS), advanced free fraud 419 (aka Yahoo-yahoo), MasterCard fraud (ATM), illegal use and software put together piracy, robbery cash piecemeal in an exceedingly fallacious manner.

At the beginning, agree to us to acceptable draw round ‘cyber crime’ and make a distinction it beginning ‘conventional offence’. CPU offense will engage illegal behavior that square measure ancient in character, like felony, scheme, fake, slander, and monkey commerce, all of that quadrangle measure topic to the legal code. The ill-treatment of computer has as well born to a

"© Daffodil International University"

gamut of recent age crime that four-sided figure calculate address by the Information Technology Act, 2006. determining cyber crime, as ‘acts that open place calculate carrying a punishment of by the information Technology Act' would be out of place for the reason that the officially authorized code in addition cover more than a few cyber crime, like electronic mail spoofing and cyber insult, cause treat e-mail etc. A force even so hard-wearing classification of computer-generated offense would be ‘illegal acts whereby the pc is what's more a gear or a objective or both'.

1.4 Significance:

Cyber and technology connected crime is on the rise and current trends indicate that it'll be a major issue in People's Republic of Bangladesh. It’s by now be see that a glomming danger become able to be seen contained by the arena of information knowledge. Following the documentation recently the hack of RAB electronic computer associate degreed e-mail threats of the previous Prime Minister Area unit associate degree case in point for a small amount of them. In distinction, crime is popping into a danger to the administration itself. Due to be short of essential legislation to undertake such class of offense, cyber criminal area component just about on the in safe hands feature to commend such offense. Inside the in order and Information and Communication Technology Act.2006, there are a unit more than a few clause in opposition to crime. But this knowledge and Communication Technology act is not the concert one. on it affirms that By enacting this act, there's an opportunity to become a secure facet once committing crimes. So, considering these facts a comprehensive crime Protection Act ought to be obligatory. This report incorporates the impacts of crime in People's Republic of Bangladesh particularly focuses on the realm of non-public life, work furthermore as political views Bodies or thinkers. we tend to believe the report would facilitate all relevant considerations and particularly policy manufacturers.

"© Daffodil International University"

1.5 Research Question:

In this research, the following three questions will be tried to answer under legal framework-

1) What is right to privacy with a special emphasis on privacy in cyber crime?
2) Does constitutional protection of a right to privacy include privacy in cyber age?
3) Whether electronic surveillance is a violation of a right to privacy in cyber age?

1.6 Methodology:

Methodology and Data Sources Bearing in mind nature, analytical and empirical research method has been resorted to complete this work. Primary and secondary sources of data have been taken into consideration for the purpose. The references have been adopted from national and international updated statutes, books of famous writers, articles published in credible journals, decided cases, research reports, acts, newspapers and websites etc. In course of this research, some renowned cyber jurists and computer engineers have been interrogated to know their views about cyber crimes and cyber-related technical & legal issues.

"© Daffodil International University"

Chapter 2

CYBER CRIME IN BANGLADESH

2.1 Introduction:

Cybercrime has been delineated by several because the "fastest growing white collar crime". It price the U.S.A. financial system regarding $ twenty four.7 billion throughout 2012; the price to a people financial system is report to be £ one.3 billion yearly; while it's price the South African financial system regarding R1 billion in a year fraud crime gift advanced challenge for sufferers, the enforcement officers (police) and lawmaker. The increase in of identity crime additionally places of interest the necessity for sufficient laws mandate tighter safety measures by business and organizations that accumulate and trade individual data.[10]

2.2 Defining cybercrime:

Cybercrime will generally be outlined as a criminal activity involving associate data technology infrastructure, as well as ill-gotten access (unauthorized access)[11], ill-gotten interception (by technical suggests that of private transmissions of pc knowledge to, from or at intervals a pc system), knowledge intervention systems misuse of devices, fake and electronic deception This include something from download ill-gotten music records to theft numerous bucks from on-line bank financial records offense additionally include non-monetary crimes, like making and distribute virus on different computer or redistribution off the record commerce data on the web.[12]

At the onset, allow us to satisfactory outline ‘cybercrime' and make a distinction it from ‘conservative offense. 166 pc offense will engage illegal behavior with the purpose of square measure ancient in natural world, like breaking and entering, deception, fake, insult, and

[10] file:///E:/New%20Folder%20(2)/THISIS/Downloads/Documents/introduction.pdf, Last visited 30 June 2010].

[11] file:///E:/New%20Folder%20(2)/THISIS/Downloads/Documents/introduction.pdf, Last visited 30 June 2010].

[12] file:///E:/New%20Folder%20(2)/THISIS/Downloads/Documents/introduction.pdf, Last visited 30 June 2010].

"© Daffodil International University"

misbehavior, all of that square measure subject matter to The legal code. The ill-treatment of computer has as well intuitive to a range of most recent age crime that four-sided figure determine self-address by the data Technology Act, 2006. technique cyber crimes, as 'acts that unit of measurement punishable by the data Technology Act' would be inappropriate as a result of the code to boot cover many cyber crime, like electronic mail spoofing and cyber insult, exploit treating e-mail etc. a impel however sturdy meaning of offense would be 'unlawful acts whereby the laptop is either a tools or a target or every.[13]

2.3 How Cyber crime occurs?

Cybercrime because the method whereby someone wittingly transfers or uses while not lawful authority a method of identification of another person with the intent to commit or to avoid or assist any unlawful activity that constitutes a violation of federal law or a crime in terms of any state or native law. Crime happens once somebody lawfully obtains the private data of another individual while not their data to commit larceny or fraud. It involves the employment of another individual's personal data for wicked functions, like for economic gain; to facilitate crimes like ill-gotten immigration, terrorism, and espionage; to evade criminal sanctions or apprehension by motion as another person (criminal identity theft) or to fraudulently get medical services (medical identity theft). different sorts of business enterprise crime embrace tax crime, wherever the crime uses the victim's personal data to get government documents or edges within the victim's name or to commit utility fraud.[14]

These criminal acts will be committed while not the help of technical suggests that likewise as involving the impersonation of a pc user's data on-line. Anyone will become a victim of crime and one's personal data will be obtained by identity thieves through things like misplacing one's case or Smartphone or from subtle scams like email phishing or by criminals prying victims' trash bins or accessing data through unsecured websites.[15] The crime can create the victim liable to crime.

[13] file:///E:/New%20Folder%20(2)/THISIS/Downloads/Documents/introduction.pdf, Last visited 30 June 2010].

[14] See 18 USC s 1028(a)(7). Also, see Pierson 2007 CILW 22; FBI 2014 <http://goo.gl/TWBoep; Hoofnagle 2007 Harv J L & Tech 98-122; Lynch 2005 Berkeley Tech LJ 260>

[15] See Perl 2003 J Crim L & Criminology 177-181 for a detailed discussion about these types of identity theft.

"© Daffodil International University"

The crime obtains very important data like identity numbers (social security, medical care numbers, addresses, birth and death certificates, passport numbers, monetary account numbers like MasterCard numbers, passwords, phone numbers and biometric knowledge (like fingerprints). This data is employed lay alia to open bank accounts, get credit and buy merchandise and services within the victims' names. so the crime will rack up large debts within the victims' names. data like the date of birth associated address will assist the wrongdoer to avoid verification processes like the employment of biometric data as an identification tool.[16]

2.4 Different types of cybercrime: It is further subdivided into the following four categories:

1) Cybercrime against individuals.
2) Cybercrime against property.
3) Cybercrime against organization and

This crime can be broadly defined as criminal activities using information and communication technology including the followings, which can be committed against the above-mentioned groups:

2.4.1 Cybercrime against individuals:

1) **Hacking or Cracking:** Hacking could be a straightforward term which suggests extrajudicial intrusion into a computing system while not the permission of owner/user.
2) **E-mail Spoofing:** A spoofed email is one during which e-mail header is cast in order that mail seems to originate from one supply however really has been sent from another supply.
3) **Spamming:** Spamming means that causing multiple copies of unsought emails or mass e-mails like chain letters.
4) **Cyber Defamation:** this happens once defamation takes place with the assistance of

[16] See FBI 2014 http://goo.gl/TWBoep; Savirimuthu 2008 JICLT 121 (where the writer argues that we require a better understanding of the interactions between data, devices, and networks before we can introduce regulatory tools to curb practices like identity theft);

"© Daffodil International University"

computers and or the web. e.g. if somebody publishes calumniatory matter regarding somebody on an internet site or sends e-mails containing calumniatory info.

5) **Harassment & Cyber Stalking:** Cyber Stalking means that following each move of a private over the web. It are often finished the assistance of the many protocols out there like email, chat rooms, user web teams etc.

2.4.2. Cyber crime against property:

1) **Credit card fraud:** Credit card fraud could be a wide-ranging term for crimes involving fraud wherever the criminal uses your MasterCard to fund his transactions. MasterCard fraud is fraud in its simplest kind. The foremost common case of MasterCard fraud is your pre-approved card falling into somebody else's hands.[17]
2) **Intellectual property crimes:** These embrace software package piracy: extrajudicial repetition of programs, distribution of copies of software package, copyright infringement: emblems violations: stealing of laptop ASCII text file.
3) **Internet time theft:** This connotes the usage by Associate in Nursing unauthorized person of the web hours acquired by another person. In might 2000, the urban center police in remission Associate in Nursing engineer WHO had abused the login name and countersign of a client whose net affiliation he had established. The case was filed underneath The Indian legal code and also the Indian Telegraph Act.[18]

2.4.3 Cyber crime Against Organizations:

1) **Virus attack:** A bug could be a bug that may infect different laptop programs by modifying them in such some way on embrace a (possibly evolved) copy of it. Viruses are often file infecting or poignant the boot sector of the pc. Worms, not like viruses, don't would like the host to connect themselves.
2) **E-mail bombing:** Email bombing refers to causing an oversized range of emails to the

[17] Rohas Nagpal, Cyber Terrorism in the Context of Globalization, ibid, p.36.

[18] Rohas Nagpal, Evolution of Cyber Crime, ibid, p.25.

"© Daffodil International University"

victim leading to the victim's electronic mail explanation (in container of Associate in Nursing human being) or packages servers (in case of an organization or Associate in Nursing piece of mail repair supplier) blinking. E-mail violence could be a kind of denial-of-service attack. A denial-of-service attack is one during which a flood of knowledge requests is distributed to a server, transportation the system to its knees and creating the server tough to access.[19] A British adolescent was cleared of launching a denial-of-service attack against his former leader, in a very ruling underneath the united kingdom laptop Misuse Act. The adolescent was suspect of causing five million e-mail messages to his ex-employer that caused the company's e-mail server to crash. The choose control that the united kingdom laptop Misuse Act doesn't specifically embrace a denial-of-service attack as a criminal offense.

3) **Salami attack:** These attacks unit of measurement second-hand for commit monetary crime. The key in here is to form the change as a result unimportant that for the duration of a} very on its own glasses case it'd go completely safe and sound. For example, a bank worker insert a plan, into the bank's servers, that deduct a lay a hand on quantity of money (say Rs. a combine of a month) from the financial credit of each customer.

4) **Information diddling:** One all told the foremost ordinary types of laptop CPU offense is info diddling -unlawful or unofficial information modification. These change know how to take place ahead of time all through information contribution or previous to production. Information diddling cases have precious bank, payrolls, register proceedings, acknowledgment proceedings, college transcript and practically all absolutely special types of development well-known.

2.5 Present situation of cybercrime in Bangladesh:

Development of Science and ICT depends on the growth of the telecommunication sector. This sector remains underdeveloped thanks to be short of liberation and unlock rivalry. The influence

[19] Rohas Nagpal, Cyber Terrorism in the Context of Globalization, ibid, p.27.

"© Daffodil International University"

of offence isn't dire People's Republic of Bangladesh as a result of money transactions haven't however been totally expedited in on-line[20]. As presently as money transactions are allowed on-line pc crimes can increase at Associate in Nursing extraordinary speed except the administration acquire the paraphernalia and communications to stop, sight and put on trial them.

However our administration at a standstill not conscious of the very information. Net armed forces provide through of the native space system are liable to alike assault and intrusion by cybercriminal a lot of typically once the protection level is insufficient. Currently every day in People's Republic of Bangladesh a few folks propel hateful Email to totally dissimilar overseas political operation and alternative V.I.P. that typically reason a significant downside for the law enforcement and conjointly for the government[21]. A number of folks use the web for sending fake and hateful data. A number of them use the web for girls and child smuggling. Porn is one more hazardous business stick of cybercriminals. However In spite of this, the government of People's Republic of Bangladesh isn't alert.[22]

2.6 Use of Internet in bad Intention:

There are two side of a make something your own. Similarly, the web conjointly has benefits and downsides. The web will be used as a accumulation damaging stick. By victimization net rebel will devastate one country. a couple of weeks alone People's Republic of Bangladesh government obligatory a restriction on gap YouTube video website as a result of it contains Associate in Nursing sound recording of a March one stumble upon sandwiched between annoyed military officers and also the head of the government. The video recording was created on March one throughout Associate in Nursing moving convention at the Dhaka camp. Many officer were gift, agitated when the paramilitary troopers savagely killed over fifty members of the military, together with several of the leaders of the People's Republic of Bangladesh Rifles border force. People's Republic of Bangladesh management says ahead of medium that YouTube has been locked within

[20] Information and Commission Technology Act, 2006 s 69

[21] ibid s 69

[22] ibid s 69

"© Daffodil International University"

the attention of countrywide safety.[23]

2.7 Bangladesh is in Danger:

The government of Bangladesh statistics for crime don't seem to be exceptional, however district judges are scepter to do suitcases in relation to the legal system and code of criminal procedure. The restricted range of cyber criminals understood is restricted to electronic mail pressure. In step with a administration learn conduct by the People's Republic of Bangladesh pc Council, only 0.3 p.c of the overall population own computers and zero.7 p.c have access to the web. In Gregorian calendar month 2007, most net service suppliers (ISPs) in People's Republic of Bangladesh to be tormented by the Denial of Service (DOS) hit. An outsized quantity knowledge of information} packets was transmit from Associate in Nursing yank data center and caused server failure, speed the performance of just about all ISPs. The attack was ab initio tried on one ISP, international Access restricted (GAL). Such Associate in Nursing attack causes serious harm. However our government remains silent when the attack and aforesaid ahead of media that we've nothing to try and do.

2.8 Bangladesh is not safe from cybercrime:

Cyber terrorists are terribly knowledgeable. It’s unacceptable for the traditional law enforcement to catch them.[24] Cyber fighting could be a advanced facet of the fashionable war, however it's not a brand new element. It has been known as by numerous name within the long-ago - intellect and EW. a number of the cyber conflict concept are illogical, like conveyance a the social order to its lap from beginning to end. Associate in Nursing out of the ordinary electronically disturbance to bank system or interchange management network.

[23] ibid s 70

[24] New age (March14, 2008), [http://www.newagebd.com/2008/mar/14/index. / last visited on 01 Jun 2010].

"© Daffodil International University"

Revolutionary teams teach their employees for upcoming cyber conflict. Terrorist organization conjointly use the web to focus of their consultation while not looking on undisguised mechanism like broadcasting, TV, or the journalists. The energy of our nation isn't at a standstill residential. They are not knowledgeable similar to yank national government department of analysis. That is why it simple for the cybercriminals to commit a criminal offense in People's Republic of Bangladesh. In our state, we tend to at a standstill don't have any cyber law conjointly. Currently every day in People's Republic of Bangladesh heaps of individuals uses of Face book on the web. The Face book could be a societal function that connect individuals. Students in a Venetian blind follower of the face book. Students using of the Face book the best part day of the week extended. Their footage, through this website friends. Downside is a few folks used face book rationale. They place of duty banned belongings and promote them on the Face book. They request student to hitch such a large amount of pretend clubs. Invitations students' community to return and be part of otherwise restricted cabaret of Dhaka town. Student community becomes influenced by this kind of promotion. such a large amount of crimes have occurred already through face book the university strictly restricted their students to open face book within the pc research laboratory hampered the education of the scholars.[25]

Organized crime is primarily concerning pursuit and may be unstated in full general as a continuance of big business by illegal revenue that. Criminal organization don't seem to be the sole play rosin illicit markets, however they're typically the foremost vital not least owing to the supplementary "competitiveness" that's provide by the danger of well thought-out aggression. Moreover, illegal organization have a propensity to be extraordinarily well-dressed at ecological scan surrounded by the look through approximately for new illegal enterprise and behavior. for the duration of this conditions, the network and also the continual enlargement of electronic business make available enormous new opportunity.

[25]Media and cyber laws- Barrister Ahmed Ehsanul Kabir p 226

"© Daffodil International University"

2.9 Impacts of cybercrimes in Bangladesh:

Many people and corporations have fall wounded to fraud. It cause trouncing to customers, creditor, money establishments and also the economy as an entire. It's been reportable by the agency Comp scan that fraud prices the South African financial system concerning R1of the billion in a year. On the other hand no billion concerning bill in our country. In step with the North American country Federal Trade Commission, fraud could be a major subject of client complaints.[26] Fraud value the yank economy concerning $24.7 billion US dollar throughout 2012, while it prices the British financial system concerning £1.3 billion each year. That time associate in Nursing cash spent responding to an fraud incident are intensive. Money establishments die the victims to clients with the answer that customers find yourself payable superior significance charge. Fraud has to be the possible to break off downward ancient spatial barrier for offense and it involving several jurisdiction. The rise in fraud offenses subsequent cyclone Katrina within the U. S. make obvious that's the situation of a significant disaster and change in human being situation will in a straight line have an effect on offense pattern. Wounded suffer by losses embrace hurting and pain, emotional harm, money sufferers, pestering from money owing collector of the creditors, the negative response of application for loan and finance bond from money establishments, harm to reputation and potential take into custody for the personality criminal alternative offence. Wounded have a medical condition hurt of their reputation as a results of against the law behavior dedicated in their name. They do not usually find out the offense till when a while has accepted, and it should receive the sufferers an extended moment in time to apparent their names and praise the past. They're sometimes unsure on however their personal information was purloined or UN agency scarf their individual data. The deception sometimes goes unobserved because the wounded seldom information the offense to the enforcement agencies[27].

Economic establishments are indisposed to description such offence as they're distressed concerning dangerous subject matter, the trouncing of their reputation and also the defeat of public self-confidence. This lack of enthusiasm is displeasing as powers that be and enforcement agency

[26] Media and cyber laws- Barrister Ahmed Ehsanul Kabir p 228

[27] ibid 230

"© Daffodil International University"

ought to be tepidly enlightened concerning such assault on company[28] IT system so as to help their considerate of and training in opposition to against the law behavior on the web. The issue relating to correct types of on-line classification has conjointly combined the confirmation of users in excess of the web. Subtle recognition gear like of biometric data are thought-about to be pricey and don't seem to be wide used. The supply of tools to commit crime has conjointly created fraud simple and profitable for offenders.[29]

2.10 Summation:

Cybercrime has be converted into a significant and on the increase downside universal, and it happens by typical earnings that and in computer network. It value the North American country financial system concerning $24.7 billion throughout 2012; the price to the British financial system is reportable to be £1.3 billion once a year while its value the South African cost-cutting measure concerning R1 billion a year. The employment of latest technology has subjected in exaggerated opportunity for victims to appropriate and illicitly use individual data to hand over Cybercrimes. It’s submitted that fraud is progressively difficult enforcement agencies and governments round the world. So it's most important to know the protecting personal identify.

[28] ibid 232

[29]ibid 233

"© Daffodil International University"

Chapter 3
PERSONAL DATA PROTECTION

3.1 Introduction:

Personal information is important thing for every person in your daily life. Every person want to protect your information from cyber attack. They won't to stolen of your data by someone. Every moment they are thinking how to protect data by theft. And they are always doing tension about this. In this chapter I briefly described how to protect personal information from cyber attack.

3.2 Defining data:

According to section 2 (Sub-section 10) of ICT Act, 2006 says that, "data" means that a design of information, acquaintance, specifics, thoughts or instructions that are being ready or are ready in an exceptionally formalized comportment, and is intended to be process, is being process, or has been process in an exceptionally CPU organization or electronic set of connections, and will be in any category as well as pc printouts, compelling or visual luggage compartment medium, knock cards, punch tapes or hold on the inside within the remembrance of the computer;[30]

3.3 Hacking personal data by computer:

If somebody, without permission of the owner or somebody, hack is an make an effort to take improvement of a ADPS or a individual set of connections contained by a pc. Simply set, it's the unconstitutional right to use to or administration over set of connections safety measures system for a few against the law function. In everyday a lots of hacker are trying to hacking data by

[30] ICT Act, 2006

"© Daffodil International University"

computer. In 2017 foreigners hacker are hacking Bangladesh bank and take a lots of money from our country.

3.4 Punishment for Hacking:

According to section 56 says that, (1) if some human being,

a) through the intention to reason or meaningful that he's likely to reason illegal defeat or damage to the municipal or an important person, will some act and in that way destroy, delete or alter any in sequence reside in a very CPU reserve or diminish its value or usefulness or affect it injuriously by any means;
b) damage from side to side unclean right of entry to any such CPU, electronic set of connections or the supplementary electronic organization with the intention of don't be in the right place to him; then such commotion shall be treat as hack offence.

(2) Whoever commit hack offence under sub-section (1) of this sector he shall be carrying a punishment of with incarceration for a term which can reach 10 years, or with fine which can make bigger to Bangladeshi monetary unit one large integer, or with each.

3.5 Cyber Tribunal Established in Bangladesh:

Bangladesh government by official notification gazette, for the object of instant and capable trial of committed crimes under the Act, be going build one or more cyber tribunal, which is sometimes stated after as tribunal in accordance with section 68(1) of the Information and Communication Technology Act. The cybercrime bench that is declared within section (1) of the section will comprise of a SJ or an ASJ are appointed by the governance with advising with the SC in Bangladesh; and such a judge assigned will be introduced "judge, cyber tribunal".[31] The cyber tribunal under the section may be given jurisdiction of whole Bangladesh or one or more session jurisdiction; and the tribunal will only judge the cases of crimes under the Act.[32] The special

[31]The Information and Communication Technology Act, 2006, s 68(2).

[32]Ibid, s 68(3).

"© Daffodil International University"

tribunal may sit and continue its procedure on a place at a certain time and government will dictate all this by its order.[33]

3.6 Cyber Appellate Tribunal Established in Bangladesh:

The Information and Technology commission Act envisages the establishment Tribunal of the Cyber Appellate at one or more situation as the governance may consider fit. According to section 82 (1) of the ICT Act, provide that the governance shall, by Official Gazette notification in the, established one or more appellate tribunals to be known as the Cyber Crime Appellate Tribunal. The govt will appoint a chairman and two members for the cyber appellate tribunal.[34] A former justice of the Supreme Court or is continuing his post or capable to be appointed as such will be the chairman and one of the member will be as an appointed judicial executive as a district judge or he may be retired and the other will be a person having the knowledge and experience in information and technology that is prescribed.[35]The members and the chairman will be in their post lowest 3 years and highest 5 years and the circumstances of their examine will be determined by the govt.[36] The Tribunal oh the Cyber Appellate shall have power to determine and hear to settling the appeal make adjacent to the order of cyber tribunal and Session court.[37] The appellate tribunal will have power of sustaining, cancel, altering, or cutting the decision of the cyber tribunal.[38] The judgment of the appellate tribunal will be fixed. The of the cyber Appellate Tribunal does not seem to be lawful with any unique power; it has been lawful with the power of a Civil Court in esteem of, interlaid,

a) Examining of witnesses and summoning

[33]Ibid, s 68(4).

[34]Ibid, s 82(2).

[35]Ibid, s 82(3).

[36]Ibid, s 82(4).

[37]Ibid, s 83(1).

[38]Ibid, s 83(2).

"© Daffodil International University"

b) Production of document Requiring
c) Evidence receiving
d) commissions Issuing and
e) Reviewing its decisions.[39]

[39]Zulfiquar Ahmed, ibid, pp.150-52.

"© Daffodil International University"

Chapter 4
CYBER LAW AND ICT ACT

4.1 Introduction:

The Information and Communication Technology Act (ICT), 2006 was the first cyber law of Bangladesh. The parliament has approved the Information and Commission Technology Act, 2006 on February and it was enacted on 8th October 2006. .

4.2 Need for Cyber Law in Bangladesh:

For the past several years, many countries have been concentrating on the awareness on questions of about the governance of cyberspace. The inquiry of who control the Internet is honestly connected to the difficulty who needs to be in charge of the Internet. From the instant that the Internet was open up to profit-making movement lots of dissimilar group sought after to control, such as consumer, announcement company, ISPs, and the administration. Of them all, the most object was the administration interference, yet it is government that have manage to put forth the most manage.

To legalize and regulate the Internet in Bangladesh, it was necessary to enact appropriate cyber law. The need for cyber law is important in our country. Because every years there are so many hackers are trying to hacking by network or social media. That's way peoples lost their identity for this hacking. To protecting of our personal identity from those hacking cyber law should be establish in Bangladesh. In recent years 2017 so many foreigners hacker are hacked Bangladesh bank account and take a lots of money. So that's the reason cyber law need in Bangladesh for protecting hacking. There are not enough laws in Bangladesh which may not punished the cyber criminals that's way more cyber laws enact in Bangladesh and punished those cyber criminals. In 2006 Bangladesh government was established ICT Act, to prevent cyber criminals in country.

4.3 Cyber Law or ICT Act of Asian country:

Cyber laws are intended to line the exact outline, some system and pointers that outlined sure commerce behavior inquiring web legal and sure contraband and therefore liable to be punished. The Information and Commission Technology Act 2006, the cyber law of Asian Nations, provides

"© Daffodil International University"

the legal framework so data isn't deprived of lawful collision, soundness or enforceability, completely on the bottom that it's within the assortment of electronic evidence.[40] One cannot look upon administration as total breakdown defensive a variety of e-commerce behavior on the firm foundation of that this deal possesses to its sky, on the other hand the law cannot be careful free ambiguity. The knowledge and Communication Technology Act (ICT), 2006 conjointly aim to provide for the officially permitted structure so legal excellence is accorded to all or any electronic proceedings and substitute behavior chosen by electronic suggest that. The Act state that if not or else joint, connect amount receipt of agreement could also be spoken by electronic suggest that of communiqué and consequently the identical have officially authorized soundness and enforceability. Some places of interest of the Act has been particular below:

Chapter I of the ICT Act 2006 specifically defines some term that is employed within the ICT sector and cyber legislation for clearing the construct. This chapter conjointly stipulates the jurisdiction and advantage of the Act. Extra-regional impact of the Act has been mentioned within the chapter.

Chapter II of the ICT Act details regarding Electronic Governance and provides entomb alia amongst others that wherever any law provides that data or the other matter shall be in writing or within the typed or written kind, then, however something contained in such law, such needs shall be deemed to possess been glad if such data or matter is rendered or created offered in associate degree electronic form; and accessible therefore on be usable for a subsequent reference.

Chapter III of the ICT Act, 2006 detail for submission to the acknowledgment, and transmit of electronic proceedings of among those parties.

Chapter V of the aforesaid Act provides a theme for instruction of certify the system. The Act envisage a manager of certify the system. Who shall execute the function of exercises course in excess of the behavior of the certify establishment as conjointly bountiful confinement down principles and circumstances leading the certify establishment as conjointly specify the diverse form and happy of Digital autograph certificate. The Act acknowledge the requirement for

[40] Zulfiqar Ahmed, ibid, p.53

"© Daffodil International University"

overseas certify establishment and it more particulars the varied supplies for the difficulty of a certify to issue Digital Signature Certificates.

Chapter VI of this Act details regarding applying the safety procedure, acceptance of Digital Signature Certificate, getting Digital Signature Certificate and management of personal Key. The duties of subscribers are enriched during this aforesaid Act.

Chapter VII and VIII of the ICT Act, 2006 discussion regarding penalty judgment, inquiry, decision, and penalization for varied crime. The penalties for harm to the pc, laptop systems etc. has been fastened as damages by means of compensation not prodigious Tk. 1,00,00,000 to affected persons. The Act talks of appointment of associate degree officer not below the rank of a Director to the government of Asian country or identical officer of authorities as an Adjudicating Officer WHO shall adjudicate whether or not a person has created a violation of any of the supply of the aforesaid Act or rules framed under it. The aforesaid Adjudicating Officer has been given the ability of a civil court.

Chapter VIII of the Act conjointly talks of the institution of the Cyber laws appellant court, that shall be associate degree appellant body wherever appeals against the judgment gone by the adjudicate Officer, shall be most well-liked.

Chapter IX of the ICT Act particulars regarding law enforcement servant, protection of exploit taken in straightness. The aforesaid Act conjointly propose to amend the Penal code, 1860, the proof Act, 1872, the Bankers' Books proof Act, 1891 to create them in tune with the supply of the ICT ACT.[41]

4.4 Legal response to crime in Bangladesh:

In order to facilitate e-commerce and encourage the expansion of data technology, the ICT Act, 2006 was enacted creating provisions with a most penalization of ten years imprisonment or fine

[41] Zulfiqar Ahmed, ibid, p.53

"© Daffodil International University"

up to Bangladeshi monetary unit ten million or with each. However, recently our Parliament amended the ICT Act 2006, raising penalties for cyber crimes setting a minimum of seven years imprisonment and a most of fourteen years or a fine of Tk. one core or each. The bill created offenses below sections fifty four, 56, fifty seven and sixty one of the ICT Act, 2006 cognizable and non-bail in a position, empowering law enforcers to arrest anyone defendant of violating the law while not a warrant, by invoking section fifty four of the Code of Criminal Procedure. All such offenses were non-cognizable within the ICT Act, 2006. However, all involved apprehend of the misuse of the ability by the police. The ICT Act, 2006 as amended in 2013 is clearly a superb accomplishment of Asian country within the field of cyber law.[42]

However the ICT Act, 2006 when any person are committed crime about cyber area that person must be punished under the ICT Act section 56 & 57. If those person are not committed crime in a cyber area but there are arrested by law enforcement agency they should right to appeal in a cyber tribunal within the section of 68 of the ICT Act.

[42] Zulfiqar Ahmed, ibid, p.53

"© Daffodil International University"

Chapter 5
CONCLUSION

5.1 Concluding remark:

The above circumstances it's proved that the calculable range of users within the years of century over a billion. Mostly cyber attack are increasing day by day in our country. Peoples are disappointing about those hackers. They want to protect their personal identity form the cyber criminals but they did not protect by individually. A country-wide ICT infrastructure can have to be compelled to be developed to confirm access to data by each national to facilitate authorization of individuals and enhance democratic values and norms for property economic development by victimization the infrastructure for human resources development, governance, e-commerce, banking, service services and every one types of on-line ICT-enabled Services. Enactment of Cyber law is extremely necessary. While not cyber law, it's insufferable for our government to regulate crime. Our parliament has passed such a big amount of laws. Is time to law which is cyber law? If our government passes cyber law straightaway then i feel the name of our country are redoubled ahead of the planet community. We tend to the individuals of our country as we tend to love our self. Asian nation is our homeland and that we our country can have our homeland from programmer. We'd like to prepare the seminar. We'd like to protest against the ill-gotten call of the govt.. We'll have to be compelled to create our self-perfect. In the end, I government to enact country as fast as they will.[43]

As we tend to move forward into the twenty first century, technological innovations have made-up the manner for USA to expertise new and wondrous conveniences within the however we tend to area unit educated, the manner we tend to look, however we tend tore amused and therefore the manner within which we do business. The capability of human minds is immeasurable. It's insufferable to eliminate crime kind the Internet. It's quite potential to envision them. History is that the witness that no legislation has succeeded in altogether eliminating crime from the world. The sole potential step is to form individuals tuned in to their rights and duties and more creating the applying of the laws additional tight to envision crime. Beyond question the ICT Act may be a historical step within the cyber world. Further, it can't be denied that there's a necessity to bring

[43] N. V.Paranjape, Criminology and Penology, 13th ed. (Allahabad: Central Law Publications,2008-09), p.141.

"© Daffodil International University"

changes within the data Technology Act to form it simpler to combat crime law don't seem to be created thus tight that it should retard the expansion of the business and influence be counter-productive. The legal code, 1860 was found meagerly to cater to the requirements of latest crimes rising from web enlargement. Even a number of the standard crimes like conspiracy, solicitation, securities, fraud, spying etc. area unit currently being committed through the net that necessitates a replacement law to curb them. It absolutely was within the background that the ICT Act, 2006 was enacted in Asian nation for the hindrance and management of cyber crimes. Before the enactment of this Act, the law applicable to cyber offenses was the legal code, 1860 that was enacted long back in 1860 once nobody even thought of engineering or cyber criminal. With the approaching into force of ICT Act, 2006, it becomes necessary to introduce bound of import modification in bound provisions of the legal code, 1860 as conjointly within the proof Act, and 1872, so as to satisfy the new needs of the Internet crimes.

However, the conception of crime is concerning the age of data superhighway of the present time. Today crimes area unit spreading at a menacing rate within the field of an internet communication system by intellectual criminals. Through the event of technology, crimes are developing in several ways in which and suggests that. Thus laws ought to be developed in such some way that crimes within the field of the technological arena will be controlled in AN iron hand. However no such effective legal provisions exist reception and abroad. Though' there are a unit some laws and convention, they can't be enforced thanks to some technical difficulties like procedural complexities and lack of correct execution system. Taking these blessings, the criminal's area unit occurring flagitious crimes like Hacking, causation malicious emails, spreading vulgar footage, cyber act of terrorism ill-gotten victimization of intellectual properties. It causes hurt to the privacy of people moreover as creates a threat to international peace and commonness. Currently it's the demand of your time to stop such style of crimes for keeping individual privacy moreover as international peace and security. Each country of the planet will enact effective legal provisions inside the orbit of their national boundary to safeguard cyber crimes. International organization may take necessary steps to stop cyber crimes from the Internet.

However, the conception of crime is concerning the age of data superhighway of the present time. Today crimes area unit spreading at a menacing rate within the field of an internet communication system by intellectual criminals. Through the event of technology, crimes are developing in several ways in which and suggests that. Thus laws ought to be developed in such some way that crimes

"© Daffodil International University"

within the field of the technological arena will be controlled in an iron hand. However no such effective legal provisions exist reception and abroad. Though' there are a unit some law[44]

5.2 Recommendations:

The above my consideration I think it was proved that the cyber crime is a big problem in our country. Peoples are considering day by day about their personal identity how to protect from cyber criminals. If the government is enact more law about cyber crime in Bangladesh that's way to prevent cyber criminals. Otherwise it is not possible to prevent cyber criminals in our country. Basically people are not aware about cyber crime or cyber attack. If people are got more knowledge about it then it's acquire to prevent offence. In Bangladesh there are only one Act established in 2006 which was Information and Commission Technology. This Act don't prevent cyber criminals and that's Act not possible to prevent cyber criminals. The government of Bangladesh is established more cyber law in our country then some cyber criminals are afraid to commit the crime. The cyber force is additionally required so as to observe cybercriminals. Currently a day's ton of is on the market in Asian nation World Health Organization tons regarding the web and cyber world. Associate degree not possible factor to enact country. Simply temperament of the government is enough to try and do this factor.

[44] N. V.Paranjape, Criminology and Penology, 13th ed. (Allahabad: Central Law Publications,2008-09), p.141.

"© Daffodil International University"

Bibliography

List of books:

1) P. Narayanan, *Intellectual Property Law*, **3rd ed. (**India: Eastern Law Publishing Co. Pvt. Ltd, **2007)**.
2) Rodney D Ryder, *Guide to Cyber Laws,* 2nd ed. (Nagpur : Wadhwa & Company, 2005),
3) Yatindra Singh, *Cyber Laws,* **3rd ed.(New Delhi: Universal** Law Publishing Co. Pvt. **2007).**
4) **Constitution of Bangladesh**

List of Statutes:

1) The Information Technology Act 2006.
2) The Penal Code of Bangladesh 1860.
3) The Draft Competition Act, 2008.
4) ICT Act, 2006

Journal Articles:

1) Mr. Pavan Duggal, 'Causes of Cyber', International Journal of Computer Science and Information Security,Vol. 3, No. 1(October. 2009).
2) Md. Shah Alam, 'A New Challenge For Law Enforcers', American Journal of Public Health, 94(6 951-957(April. 2004).
3) Ripon Kumar Biswas, 'Cyber crimes need more attention', Tuesday, September 09, 2008.

List of Newspapers:

1) The Daily Star
2) The Financial Express
3) The Prothom - Alo
4) The Bangladesh Observer
5) Daily Anandobazar
6) The New Age
7) Daily Ittefaq

"© Daffodil International University"

8) The Times of India
9) Daily New AGE
10) Dainik Bhorer Kag
11) Amar Desh
12) Daily Banglabazar

List of Web-Sites:

1) The Financial Express (10 January 2008), [http://www. thefinancialexpress -bd. com/ newindex. php? archive _ date=2008-01-10].
2) [http://www.naavi.org/pati/pati_cybercrimes_dec03.htm]
3) [http://www.cybercrimelaw.net/].
4) [http://www.rediff.com/search/2003/feb/18crime].
5) TheDailyStar(6September2008),[http://www.thedailystar.net/newDesign/archive.php?date=2008-09-06]
6) TheBangladeshObserver(6September2008),[http://www.bangladeshobserver.com/].
7) [http://nation.ittefaq.com/issues/2008/07/19/news0019.htm].
8) [http://www.voanews.com/english/2009-03-09-voa36.cfm].
9) Newage(March14,2008),[http://www.newagebd.com/2008/mar/14/index.html]
10) http://nation.ittefaq.com/issues/2008/11/25/news0088.htm].
11) [http://www.facebook.Com. Face book is a Social utility that's connects the people].
12) TheProthamAlo.net.bd(24August2004),[http://www.prothomalo.net/V1/newhtmlnews1/home.php?Date=2004-08-24].
13) [http://www.cnewsvoice.com/DNews.php?NewsID=N000000770 last visited on 15 July 2010].
14) TheTimesofIndia(12December2008),[http://publications.mcgill.ca/reporter/2008/12/page/2/].
15) TheAnandobazarprotika(01January2008),[http://www.anandabazar.com/archive/1080101/index.htm].
16) [http://bangladeshwatchdog.blogspot.com/2008/09/cyber-crimes-need-more-attention.html]
17) [http://issues.takingitglobal.org/onlinesafety?gclid=COvRwvaAwpcCFQRPtAodeWffSQ].
18) [http://www.cybercrimelaw.net/Cybercrimelaw.html].

"© Daffodil International University"