Cyber Terrorism Through Patient Data Theft: Is The Law Ready To Deal With It?

Dr. Rajib Kumar Majumdar,
Neurosurgeon and Medico-legal Consultant,
Faridabad, India.

Abhishek Majumdar
BBA. LLB. (4th Year), Symbiosis International (Deemed) University

Abstract
The next generation cyber attacks will be aimed at the physiological and personal data of a human being in a concentrated targeted pattern and the Law both Domestically and Internationally stands at a very weak footing. The current paper seeks to study the cause effect relationship of such cyber mal-activities and the legal frameworks which deals with it.

Keywords: **Cyber terrorism, Human physiology, Patient data.**

Introduction

World- wide ,there is an increasing shift in digitising all forms of data, whereby storing, tabulating and propagating the same in a numeric ascendency and linking the same to a common digital platform not only helps in storing huge complex data in a very limited space, but also makes it available for all sorts of consultation at the touch of a button. Theoretically, this is an utopian concept of access and reach in the shortest possible time but practically this becomes open to all sorts of prying by various individuals from a person to agencies, to most intimate likes, dislikes, sexual preferences ,transplanted organs, any specific disease etc of a private individual, more specifically, a person attending a hospital as a patient or a layman for any medical examination and accidental finding of some disorder which may not be socially acceptable, but nonetheless, a tiny occupant of a digitally stored personal data in any form whether chip based or cloud computed, can be open to access by a cyber hacker ,and in the absence of any inter-locuting International or Municipal Legal Culpability, may so manipulate the person at his own free will or blackmailing him/her into submitting some damaging information . Hospital computer systems are under constant surveillance by cyber frauds who are on constant prowl to thieve out information, manipulate records or just can cause irreparable damage to a whole treatment protocol by devitalising the data and causing innumerable harm to the patient. At Kern Medical Centre Bakersfield in July 2010[1], a severe virus attack on the hospital system completely crippled the system thereby jeopardising the life and treatment of the patients and the reputation of the hospital. The Law dealing with such a situation is quite tweaked and lame and can neither prevent nor impute any pre-emptive strike upon such a happening. The Indian Parliament passed the Information Technology Act 2000[2] following United Nations Model Law 1997[3] but does not define the term Cyber terrorism.

Cyber Attack and Cyber Terrorism- The Legal Framework Defined

There is no authentic definition of the term 'cyber attack'. At best Black's law dictionary defines 'computer crime'[4] as a crime involving the use of a computer such as sabotaging or stealing electronically stored data. 'Cyber terrorism'[5] is terrorism involving the commission of threat or unlawful attack using a computer against another computer, networks and electronically stored information and actually causing the targets to fear or experience harm.

According to Jay Dratler Jr.[6], "much of the hoopla about the 'cyberspace law' relates more to climbing the steep learning curve of the internet's technological complexities than to changes in fundamental legal principles. To the extent there was 'new law' it was almost entirely case-by-case development, in accordance with accepted and well understood basic legal principles albeit applied to new technology and new circumstances."

[1] https://www.ncbi.nlm.nihgov/pmc/articles/PMC4516335, accessed on 16/03/2018.
[2] Information Technology Act 2000, Universal Law Publishing, Lexis Nexis.
[3] https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf, accessed on 16/03/2018.
[4] Bryan A. Garner, Black's Law Dictionary, 452, (10th Edn., Thomson Reuters, 2014).
[5] Bryan A. Garner, Black's Law Dictionary, 1702, (10th Edn., Thomson Reuters, 2014).
[6] Jay Dratler Jr., Cyber Law, 1.01 at 1-3, 2001.

Cyber law is the law governing computers and internet with a supposedly international jurisdiction but when it comes to actual application there are innumerable hurdles to be conquered. It is so astounding that cyber crime is not defined in IT Act 2000, nor in National Cyber Policy, 2013 nor, in any other regulation in India. So how can a gruesome cybercrime be defined when digital information of a patient is surreptiously hacked and passed onto a competitor where the information can be used to blackmail or intimidate an individual. This can best be dealt with IPC, 1860 where in to purport a crime the two important hall marks like *mens rea* and *actus reus* when applied to cyber attack is very difficult to substantiate. According to NCRB very few cases have been registered under both IT Act and IPC and the conventions remain in single digit.[7] In India none of the existing laws give any legal validity or sanctions to the activities in cyberspace. A very pertinent example is e-mail, the most common mode of communication actually does not find a legal sanction of e-mail id meaning e-mail id is not 'legal in India'.

A very important and intriguing aspect of the jurisdiction according to IT Act, 2000 sec. 1(2) is vexatious in proposition wherein, the Act extends to whole of India and also applies to any offence or contravention committed outside India by any person (also esc. 75 of IT Act, 2000) however in the same breath, the Act propounds that it will be applied reciprocally also. However, this act is silent regarding international treaties and contraventions since, just a law without a sanction by treaties or contraventions , on an international arena is simply an aircraft without its rotors, machine or the landing gear. However, if you look at sec. 79 which provides immunities to 'intermediaries' like internet service providers etc., one can easily see that most of data stored and contradicted occurs at the intermediary level. So one has to actually enact a watertight law to get the maximum benefit of the digital technology. Steganography, Trojan, Malware, etc., are all part of digital technology and per se, not criminal but when used with malicious intent can become a difficult task to endure and correct especially as most of it has a social impact impetus.

Medical Data: What it means and how is it vulnerable to cyber attacks

A very significant achievement in medical documentation in the 21st Century has been the systemic digital encryption of the minutest details of a patient through incremental categorisation called 'Medical Bioinformatics'. Previously all the details relating to patient e.g., name, age, sex, address, personal history, professional history, genetics, etc. which were required either for treatment purpose or in medical research was either stored in written form or in the analogue storage system. Although the details sought were quite graphic as it is required for any successful treatment, the sheer voluminous manner in which it was stored made it quite immune to be detailed to a third party. Ever since medical bioinformatics developed and hospital data of patient record got stored either through, specialised softwares or software applications or more appropriately 'apps', the increased incidence of data leak through malware introduction or the app itself being an agent in transformation of details became quite a headache. It is not that hospitals or private clinics who have to get patient information and store it in their storage banks for past reference or future consultation do not use adequate safety precautions like anti-viruses and firewalling but lately through remote device interventions or increment downloading of applications which seek and get all the information they need, may itself be the main cause where patient data may be vulnerable to passover to third party. Hackers at remote locations can attack hospital computer systems, manipulate records, steal them, block them and may lead to disturbances in conduction of surgical procedures, can delay test result and simply totally disturb the settled methods of patient case. In July 2010 Kern Medical Centre at Bakersfield faced a virulent computer attack which paralyzed the system to such an extent that the harassed doctors and the nursing staff had to resort to paper pencil method of communication.[8] It so happens that hospitals are sitting ducks.

When it comes to malware attack as they are in control of a lot of data right from personal to financial including insurance details and once hacked, such an information can be a gold mine of information and subsequent nefarious activities. In the final run, a cyber threat to hospitals may act as a deterrent in confidence upon the security and privacy concerns of the patient and bad for hospital practice. In a recently conducted study by a renowned institute it has been revealed that there is a 10 thousand fold heightened attacks on digital data of hospital in the past decade and criminal attacks on medical data breach has now assumed a phenomenal proportion.[9] The main reason is that the data stolen has a good cash benefit, when sold in a black market. This has presumed the proportion in the recent days as there is a race amongst government for massive digitalization and integration without caring to put enough fool proof safe guards in

[7]http://ncrb.gov.in/StatPublications/CII/CII2015/chapters/Chapter%2018-15.11.16.pdf(accessed on 23/02/2018).
[8] http://www.bakersfield.com/ (accessed on 27/02/2018).
[9] https://www2.idexpertscorp.com (accessed on 07/03/2018).

position. This has led to an awe striking amount of information which is available on the net and is crisscrossing various internet channels without the prior information of the individual. The corollary of the internet i.e., 'Dark net'[10] has limited access to public at large but is freely available to criminals. This offers cyber criminals a virtual run over with their merchandise to trade off for pecuniary benefits, or even for spying purpose. The financial aspect of stealing the information of a patient through cyber breach of a hospital record is so phenomenal that cyber criminals have now percolated their expertise in breaking medical records of medical institutions. In an astonishing revelation by Ken Westin[11], it has been brought to the forth that most of institutions/individuals take the complexities of those transactions in a very lighter vein. So much so the governments in their utterly misplaced enthusiasm to link the security number of individuals to every services have actually baulked these very individuals' security concerns. A very common parlance adopted by cyber criminals is phishing the credit card numbers from available data, selling them off in black market where they can be easily duplicated and fraudulent transactions done without the slightest knowledge of the victim. This takes place very fast as the information which is stolen has an expiry date so, exploitation has limitation attached to it. Once the shelf life expires and the theft is discovered by the affected party, it is too late as the damage has already been done[12] and the lame duck law goes brow beating without providing any relief to the victim. In a New York Times article[13], the head of United States Cyber consequences unit gives a very grim picture of the State of Cyber security. He postulates that "persons in the various field actually take to technology to deal with this otherwise a strategic problem". These experts do not take into consideration as to who is behind the attack, what is his ulterior motive and what would be the consequences. They are only considerate about the technical glitches and how to solve them to bring the system on again. Their myopic focus on technology makes them blind to this situation where cyber criminals have out run the technology, as well as the law.

How the law deals with this morbid situation Internationally and Nationally:

Section 75 of IT Act, 2000 covers all the offences, whether committed in India or outside it. But the biggest question arises as to how to get it implemented ? It is simply because the jurisdictions under local laws and that at International level are at variance to each other. In S.S. Lotus[14] (France v Turkey) case it was defined that jurisdictional territorial definition was subject to international custom or convention. So under cyberspace criminal activities the procedural aspect of IT Act 2000 falls woefully short. The Budapest Convention first addressed the need for a global cybercriminal law but unfortunately India is not a part of it. This convention emphasised upon Internet computer crime in a very detailed manner and cyber terrorism which hitherto has not been defined in IT Act 200 is a part of this convention making this convention a very comprehensive legal entity as per the cybercrime is concerned. This Convention Theoretically lays down the fact that criminal should be uniform in cybercrime, that there should be a well defined procedure of investigation and prosecution and that there should be a well defined and effective global cooperation. This convention emphasized upon 'internet computer crime.' Cyber terrorism is a part of the convention. This convention has laid down theoretically that criminal law should be uniform in cyber crime, that there should be a well defined procedure of investigation and prosecution and that there should be an effective global cooperation. This convention has for the first time defined as to what constitutes cyber crime like unlawful access, data intrusion, etc. The various sections of IT Act, 2000 like section 70 i.e., illegal access, section 65-67B i.e., data interference etc. have a cogent reminder in Budapest Treaty at Article 2 and Article 4, 5, etc. Comparing with USA we can definitely see that American laws are far more defined with respect to cyber crime wherein crimes committed through the use of computers or in cyberspace are illegal irrespective of State. The Counterfeit Access Device and Computer Fraud and Abuse Law of 1984 and consequent correcting acts deals with all the criminal exercises executed using PC. It further strengthened the law by enacting the NIIPA (National Information Infrastructure Protection Act) in 1996. There are various laws which have been enacted in the USA to battle cyber crime, from 1984 till date when contrasted with India, with its solitary 'IT Act, 2000'. Some of the important cyber crime laws enacted by U.S.A. are Counterfeit Access Device and Computer Fraud and Abuse Law of 1984, NIIPA 1996, The Access Device Fraud Act 1984, The Computer Fraud and Abuse Act 1984, The Electronic Communication Privacy Act 1986, etc. In US internet as a means to 'freedom of speech and expression' is taken very seriously and 'net neutrality rules' prohibit internet providers from blocking or slowing down websites whereas privacy as inherent in Article

[10] https://en.wikipedia.org/wiki/Darknet (accessed on 08/03/2018).
[11] http://www.tripwire.com (accessed on 04/03/2018).
[12] http://www.verzonenterprise.com (accessed on 14/03/2018).
[13] http://bits.blog.nytimes.com/2014/12/02 /hackedv.hackersgame (accessed on 14/03/2018).
[14] S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10.

21 of Constitution of India has been only a recent development. In United Kingdom, the Computer Misuse Act of 1990 is a comprehensive computer crime legislation and is followed by Singapore as well as Malaysia.

When a common crime is committed, it is a usual practice that the criminal escapes to another country to escape liability. However in cyberspace the practice is altogether different and hence more vexed. Crime is committed from a different state upon another state where jurisdictional authorities are different and there are different laws governing it. It also becomes very difficult to extradite a cyber criminal sitting in an all together different country and hacking the hospital record in a different country to sell it at the black-market as in section 21 of Extradition Act, 1962, the accused can be tried for only those offences laid down in the extradition decree and for no other offences.

Conclusion

As it stands today, cybercrime has become a grime reality and medical theft perpetrated through internet channels a dangerous trend. The major difficulty in legal enforcement is that different countries of the world have their own individual laws to tackle the situation making it problematic to apply it on a global platform. In India balance has to be stricken between the civil aspect, the criminal aspect compromising national security.

India should become a part of the Convention on Cybercrime to get international cooperation in attacking and securing cybercriminals specifically when sensitive intimate data leak through compromised hospital software of an important individual of national security may jeopardise the national interest.

From the above discussion one thing is clear that cyber crime law is a nascent law in most of the countries because of its international presence and in India even the nascence of law is woefully inadequate. In such a languishing state of existence linking of one's security number to such intimate details can only be a catastrophic outcome. It therefore, becomes necessary that a variety of codified law as a separate existential apportion be enacted in tandem with international apparatus at the earliest.