Ethics of Cyber Forensics in India

Narayan Gupta
3rd yr, B.A.,LLB. Student,
Jindal Global Law School, Sonepat
Delhi NCR, India – 131001
Email id: ngupta98@yahoo.com

Abstract: This paper tries to understand the need for legislative changes in Technology law in India. It takes an example of Cyber Forensics used in the field of law as evidence and its conflict with individual's privacy. It concludes by suggesting an existing model of laws that could be adopted by India as a first step to solve this problem.

KEYWORDS: Technology, Cyber Forensics, Law, Privacy, Evidence

– – – – – – – – – – ◆ – – – – – – – – – –

Technology Law is still a developing area of law in India. This paper tried to highlight few important legislative changes needed to monitor the use of technology. This paper starts by defining cyber forensics in brief. Secondly, this paper will highlight the present rules or norms prevalent in India for cyber forensics. Thirdly, the need for ethics in this profession would be highlighted. Lastly, this paper will come up with a model of ethics which could be adopted in India.

Cyber Forensics is one of the branches of forensic sciences which deal with digital data. With the advancement of technology, Courts all over the world have started accepting digital data as evidence provided certain rules are followed. As any other evidence present at crime scene, digital data is also collected by crime scene investigators and then forwarded to the competent labs for analyzing it. This whole process of collecting, packaging, forwarding and analysing is crucial for a digital data to be admissible in Court of law.

Presently, there is no direct regulation in the field of Cyber forensics. For an individual to become a cyber forensics, he needs to complete a certified course on computer forensics after completing his graduation. As soon as he completes that

course, he becomes a certified cyber forensics expert whose findings can then be used in Court of Law. There is no organisation or government body which regulates the entry in this profession. Also, there is no binding code of conduct for people working in this profession. Ideally, only a sample of the collected evidence is being sent to the respective lab for analysing it but in cases of digital data, the evidence in entirety is being sent for examination. The problem with this is that, if in any circumstances, the court wants to get the evidence examined by a second expert, it would not serve the purpose of justice as digital data is easy to manipulate. Also, crime scene investigators are not trained to collect digital data. For instance, when a computer is found switched on, the data stored on RAM can help in solving the crimes but due to lack of skills, usually, crime scene investigators turn off the computer and send it to Forensic Science Laboratory for examination.

Considering the fact that the primary use of a cyber forensics, as of now, is in law enforcement agencies to deliver justice, there is a need of a regulatory body which could make sure that all the people entering this profession are actually qualified to do their task. With the increase in use of internet, there is a gradual increase in cyber crimes as well. Many-a times, Judgment of the court to convict or acquit someone solely relies on the evidence which is in form of Digital data before it and since judges or lawyers are not competent enough to analyse the digital data, they have to solely rely on the testimony of the cyber forensics expert. For instance, if a person receives obscene images from a stranger despite of clear rejection, the sender could be charged for stalking under Indian Penal Code. In these types of cases, the sole evidence before the court is digital data. What if the cyber forensics analyst mishandled the evidence which led to wrong conclusion. What would happen if the software or tool used for analysing the data used by cyber forensics analyst is not

reliable. To answer all these questions, there is a need of a regulatory body which could set uniform standards and process of functioning for all cyber forensics analyst.

According to me, Right to privacy which is a fundamental right guaranteed to every citizen of India by Constitution of India is being infringed when digital data is being given to a cyber forensics analyst for analysing. Whenever any person authorised by law comes with a search warrant and seizes any gadget which is suspected of having any electronic evidence, the person not only takes the evidence which is necessary for the particular case but also gets access to the other confidential data stored on the gadget. Not only the investigating officer but also the cyber forensics analyst can use the other confdential data present on the gadget for other purposes. This is similar to the concern raised by people on making Aadhar Card mandatory in India. When Unique Identification Authority of India (UIDAI), on behalf of Government of India collects bio metrics of every citizen of India, they are actually infringing right to privacy of an individual. If any unauthorised person gets access to the central database of fingerprints collected by the government, it won't be much difficult for that person to misuse that fingerprint. Considering the fact that the collection of fingerprints is being outsourced by government of India to private entities, even if an authorised person gets access to it, there are high chances that he/she can misuse the accessible information.

According to National Crime Record Bureau, there is an increase of 65.3% in cases of cyber crime being reported in 2014 as compared to 2013[1]. Though there is no empirical research on as to why there ia an increase in cyber crimes in India but one

[1] Data available at official website of National Crime Records Bureau (NCRB) (http://ncrb.gov.in/), CRIMES IN INDIA 2014, *Chapter 18, Cyber Crimes*, last accessed at 27 October, 2015.

of the reasons could be no regulations on cyber forensics analyst. National Crime Record Bureau also states that around 52.7% of the offenders under IT Act were in age group of 18 yrs to 30 years. Though all the computer engineers and cyber forensics analyst are taught things like hacking to help law enforcement agencies in delivering justice but not every person who has gained this knowledge through a certified course ends up getting a job in Forensics Science Laboratory. Many of them might have turned them into cyber criminals. The other issue which can be noticed through the national crime record bureau report is that only 4246 people were arrested out of 7201 cases being reported. This depicts the inefficiency of Indian Cyber cells to solve the cases. The reason could be anything, it could be mishandling of evidence or wrong findings by cyber forensics analyst.

All the above raised issues depict that there is a need of code of conduct which stops people from engaging in unethical conduct in profession of cyber forensics in India.

With the rising increase in cyber crime all over the world, some organizations have come up with a code of conduct which every individual who obtains a certificate of computer forensics has to abide by. If any violation of any provisions of code of conduct is being noticed, his/her certification is cancelled. For instance, *The International Society of Forensic Computer Examiners (ISFCE)* have a good model of code of conduct which can be adopted by everyone. ISFCE is one of most reputed organization in the field of computer forensics whose certification, also called as Certified Computer Examiner (CCE), is accepted in many countries. In order to get its certifications, one needs to be get training at its authorized training centre and have an experience of 18 months in analysing digital evidence. Once a person becomes a

certified computer examiner, he/she has to abide by the code of ethics laid down by ISFCE. Its code of ethics[2] states that a CCE will at all times maintain the utmost objectivity in all forensic examinations and accurately present findings; conduct examination based on esatblished, validated procedures; abide by the highest ethial standards; testify truthfully in all matters before any court, board or proceedings; thoroughly examine all evidence within scope of engagement, etc. It also states that Certified Computer Examiner will never withhold any relevant evidence; reveal any confidential matters or knowledge learned in an examination without an order from a court of competent jurisdiction or with the express permission of the person whose gadget is being confiscated; express an opinion of guilt or innocence of any party; engage in any unethical or illegal conduct; misrepresent education, traning or credentials, show bias or prejudice in findings or examinations, exceed authorization in conducting examinations.

In my opinion, in a country like India where popular projects like Digital India have been initiated, there is a urgent need of a legislation or a regulatory body which ensures quality and maintains certain standards followed by certain code of conduct similar to that of the International Society of Forensics Computer Examiners.

[2] Code of Ethics available at https://www.isfce.com/ethics2.htm , last accessed at 27 October 2015.