Perry4Law
An Exclusive Techno-Legal Corporate, IP & ICT Law Firm

New Delhi, India

Cyber Forensics Trends And Developments In India 2013

The Cyber Law Trends and Developments of India 2013 (PDF) and Cyber Security Trends and Developments in India 2013 (PDF) have already been covered by Perry4Law and Perry4Law's Techno Legal Base (PTLB). In this research work we are covering the Cyber Forensics Trends and Developments in India 2013. Our readers can read more about Cyber Forensics at the Computer Forensics Research Centre of India managed by PTLB and our Cyber Forensics Linkedin Group that is Open Group. Some of the significant Trends and Development in this field in 2013 are as follows:

(1) Cyber Forensics In India: Cyber Forensics in India has failed to take up a shape in the year 2013. Although many Good Policy Decisions were undertaken by Indian Government regarding establishing Cyber Forensics Capabilities in India yet these Policy Decisions failed to materialise. However, there is

(2) Cyber Forensics Skills Development: Indian Government has been stressing upon Skills Development in India for long. Even a budget allocation of Rs 1,000 crore has been made in favour of Skills Development in India. However, Techno Legal Skills Development in India is still to be achieved. In these circumstances, the Computer Forensics Trainings in India is urgently required.

(3) Cyber Forensics Education In India: A growing number of Educational Institutions, Colleges and Universities are now providing Cyber Forensics Education in India. Although the courses provided by these Educational Institutions are "Basic Level Courses" yet that is a good beginning. Further, these Educational Institutions must stress more upon Skill Development rather than a Degree. More Skill oriented Cyber Forensics and Information Technology Courses must be introduced in India. The scope of Computer Forensics Exams and Courses in India is going to increase in future.

(4) Increased Cyber Crimes In India: There has been a great surge in the commission of Cyber Crimes in India. However, Law Enforcement Agencies of India are not well equipped to deal with the most basic Cyber Crimes. Sophisticated Cyber Crimes are well beyond the Capabilities the Cyber Crime Cells in India. Police Officers in India need to be trained in the fields of Cyber Crime Investigation, E-Discovery and Cyber Forensics. Further, Constitutionally Sound and Law Abiding Law Enforcement Technology in India must also be developed by Indian Government.

(5) Cyber Crimes Investigation In India: Cyber Crimes Investigation in India are performed in a very "Casual and Unprofessional Manner". Recently the Central Bureau of Investigation (CBI) committed a Cyber Forensics Blunder in Aarushi Talwar's Murder Case. Too much emphasis is given to the Internet Protocol Address (IP Address) that cannot be the "Sole Ground" of Arrest and Conviction. In some cases "Wrong Imprisonment" of innocent people has also taken place in India due to incorrect IP Address tracking and defective Cyber Crime Investigations. E-Discovery and Cyber

Forensics Processes must be essential parts of Cyber Crimes Investigation in India that are presently missing. In fact, a Public Interest Litigation (PIL) has been filed in Supreme Court of India to direct the Indian Government to frame Regulations and Guidelines for Effective Investigation of Cyber Crimes in India.

(6) Cyber Forensics Best Practices In India: There is no second opinion that Cyber Forensic Investigation Solutions in India are needed. These Solutions must be Techno Legal in nature and they must cover the Hardware, Software, Regulatory and Policy issues. We have no Cyber Forensics Best Practices in India that are adopted by law Enforcement Agencies while conducting various Investigations. In fact, lack of use of Cyber Forensics Best Practices in IPL Match Fixing Case may jeoparadise it. Further, Forensics Analysis of Nokia's Computer used to download software in India was also not performed properly.

(7) E-Mail Policy Of India: Foreign Companies and Websites are not complying with Indian Laws and demands of Law Enforcement Agencies of India. Even the United State's Government has refused to serve Summons upon Companies incorporate there and blocked the MLAT attempt of Indian Government.

The Delhi High Court is analysing E-Mail Policy of India and complaint mechanism to Facebook. E-Mail Service Providers like G-Mail are abetting and encouraging commission of Cyber Crimes as well. E-Mail Service Providers like G-Mail, Yahoo, Hotmail, etc are also facilitating violating the provisions of Public Records Act, 1993 wherever Public Records are involved. In order to expedite the Cyber Forensics Investigations, the Servers of these E-Mail Service Providers must be located in India. Otherwise, the services of these E-Mail Service Providers must be banned in India. In the present circumstances, performing even basic level Cyber Crime Investigations and Cyber Forensics exercises is not possible as Foreign Companies do not cooperate at all.

(8) Registration Of FIR Obligatory: As per the Judgment of the Supreme Court of India, Police Must Register FIR for Cognizable Offences in India Compulsorily. A Constitution Bench (PDF) of Supreme Court of India in *Lalita Kumari v. Govt Of UP (2013) SC (5J) (PDF) held* that police officers are bound to register FIR upon receiving information of commission of a cognizable offence in India. This would also means that Police in India would now need to tone up its Cyber Forensics Skills to successfully investigate many Traditional and Cyber Crimes.

(9) Bitcoin Crimes Investigations In India: The Legality of Bitcoins in India was always in Doubts. The Reserve Bank of India (RBI) cautioned users of virtual currencies against various risks. These include Legal Risks as well. The Enforcement Directorate (ED) searched two Bitcoins websites and their offices. ED believes that Bitcoins money can be used for Hawala Transactions and Funding Terror Operations. In the present Non Compliance Environment, more such Searches and Arrests are anticipated. Enforcement Directorate (ED) must use E-Discovery and Cyber Forensics Methods to detect possible Legal Violations by Bitcoin Websites.

(10) Money Laundering Investigations In India: Of late cases of Money Laundering and Banking Frauds are on rise in India. For instance, ICICI, HDFC and Axis Banks were alleged to be indulging in Money Laundering and Benami Transactions. The Finance Ministry and RBI even investigated Money Laundering accusations against ICICI, HDFC and Axis Bank. At present these violations are taken very lightly by the Finance Ministry and RBI. But with the plan to establish Income Tax Overseas Units (ITOUs) of India in Foreign Countries this casual approach would be abdicated and sound Cyber Forensics Capabilities would be required to be possessed by the Tax and Revenue Officials to successfully prosecute the culprits.

(11) Serious Frauds Investigation In India: Serious Frauds Investigations in India have received a boost by the enactment of the Indian Companies Act, 2013 (PDF). Now the Serious Frauds Investigation Office (SFIO) has been conferred wide powers by the new Act to deal With Corporate Frauds, Economic Offences and White Collor Crimes. The Ministry of Corporate Affairs (MCA) has also issued some Rules under Chapter XIV of Indian Companies Act, 2013 pertaining to Inspection, Inquiry and Investigation by Indian authorities and SFIO. The Suggestions Regarding Rules Pertaining to Inspection, Inquiry and Investigation (SFIO) by Perry4Law (PDF) has already been provided by us in this regard. Cyber Forensics Skills and use of E-Discovery can greatly help SFIO in achieving the wider Duties and responsibilities assigned to it by the Indian Companies Act, 2013.

There are many more aspects that we wish to discuss these Trends but due to the limited scope of this work, we are restraining from doing so. Perry4Law and PTLB hope that our readers would find this Trend useful.