Collection of electronic evidence from internet service provider and it's admissibility in the court: An analysis with reference to cybercrime.

Rajesh Kumar

Research Scholar, Chanakya National Law University, Patna.

Abstract:
Electronic evidence plays a vital role in dealing with cyber crime. Usually, Electronic evidences are available in digital storage devices or are preserved by the service providers of digital platform (i.e. Internet Service Providers etc.). There are several authorities involved in these data generation process and evidence presenting before the court. The law enforcement agencies have no easy access to the service provider's server. Therefore, collection procedure of electronic evidences from internet service provider, their admissibility and appreciation before the court is always a challenging issue. The data authenticity and integrity has always been questioned. A lawful access to the server of service providers for law enforcement agencies can omit the involvement of different authorities and resolve the issues of authenticity and integrity of electronic evidences before the court of law.
***Keywords*: Electronic Evidence, Internet Service Provider (ISP), Law enforcement Agency (LEA), Cyber Crime, Police Investigation.**

I. Introduction:

Over the time, crime has been changed their nature and pattern. In ancient time, blood, bones, knife or iron rod was used as evidence in crime before the court. But, today apart from these evidences, electronic evidence has been played an important role in decision of conviction or acquittal in every crime. Electronic evidence or digital evidences as usually available in digital storage devices (which is usually found at the scene of crime) and data (electronic evidence) preserved by the service providers of digital platforms. For example: Internet Service Provider, Mobile Service Provider, Email Service Provider, Web Service Provider etc. Electronic evidence is fragile in nature and can be easily altered, damaged or destroyed through improper conduct or examination. Therefore, identifying, collecting, preserving and examining electronic evidence requires special care.

Data extraction of digital storage devices has been performed by the electronic examiner of forensic science laboratory. Therefore, integrity and authentication of such electronic evidences are mostly unquestioned before the court. On the other hand, data (electronic evidence) provided by the service providers are always rising questions on their integrity and authenticity. With the increasing use of cloud computing, where data is stored on data centre's servers and there is a continuous exchange of data, collecting and preserving electronic evidence and its admissibility in a court of law is a difficult task. It is also a legal issue.

a. Concept:

The collection, protection and presentation of electronic evidence are a core part of cybercrime investigations. Electronic evidence plays a decisive role in every conviction or acquittal and is highly appreciated by the Court. Therefore, during the course of investigation, the police try to follow all the standard operating procedures for collecting electronic evidence from the Internet Service Provider. User data is preserved by Internet service providers, provided as per the requirement of law enforcement agencies.

b. Statement of Problem:

Preservation of data (electronic evidence) by Internet service providers and their presentation before court by law enforcement agencies is a common occurrence. But, their authenticity, integrity and appreciation are always questioned in court due to the involvement of multiple authorities in data acquisition. According to 65B of the Indian Evidence Act 1872 "electronic evidence must be produced by the system administrator of the server", otherwise it would not be admissible in a court of law. But, in practice Server System Administrators of Internet Service Providers are never present; Nodal Officers are rarely present before the court. Police officers (law enforcement agencies) usually present electronic evidence in court, which has no role in data acquisition. Due to which electronic evidence is not being appreciated before the court.

c. Objective:

The main objective of this research paper is to provide law enforcement agencies with solutions for limited, customized and easy access to the server of internet service providers. The authenticity and integrity of the data access from the service provider's server is admissible before a court of law. Therefore, the researcher will try to explore the issue and find the scope to establishment the integrity and authenticity of electronic evidence provided by service provider.

d. Scope:

The researcher has tried to explore the scope of research to find out the solution of issues related to authenticity, integrity and admissibility of electronic evidence in the court of law.

e. Literature Review:

The apex court enlightens and appreciating the digital evidence whiles the delivering of judgment in Mohammad Ajmal Amir Kasab Vs. State of Maharastra ors, the court consider the call details records, call interception, intercepted communication over VOIP (Voice over internet protocol) and IP addresses as electronic evidences.[1]

Pawan Kumar Shrivastva in his article "Electronic Evidence in Crime Investigation - Darknet & Policing" states that: The integrity, authenticity and admissibility of electronic evidence before the court is a major challenge in India as there has been ambiguity regarding the requirement of authentication of electronic evidence under section 65B of the Indian Evidence Act 1872. In case of T.S.Dighole v.Manik Rao Shivaji Kokate, the apex court of India also observed that "As compared to the traditional evidences, the electronic evidence should be more accurate and stringent".[2]

1. (2012) 9 SCC 1
2. (2010) 4 SCC 329

Bivas chatterjee is in his article Cyber Laws and Appreciation of Electronic Evidence: Challenges told that "India is the largest internet user country and people all over India are using WhatsApp, Facebook and many other online sites and transacting in various e-commerce sites. Therefore, a lot of evidence in the cyber space is found in digital form and all of them are admissible, if collected and presented in a proper way".[3]

II. Collection of User data and Internet Service Provider:

Service providers are preserved the data (Electronic Evidence) of user. Depending on the nature of service the providers are collected data of the users. There are two types of user data preserved by the service providers: User generated data[4] & Service providers defined data.

a. **User generated data (Electronic Evidence):**[5]
   Every user has created their own data on social media and other digital platforms. Such as: Images files, Audio, Video, Text, Document, Web pages, Databases, Subscribers records, social media postings. These data can be used as electronic evidence in crime investigation.
   Users created data are usually available in open source. To gather such information, open source tools and subscription based tools are available. These information as electronic evidence has been presented by the investigating agencies along with certificate under section 65B of Indian Evidence Act 1872.

b. **Service providers defined data (Electronic Evidence):**
   The service provider has preserved various data as required to maintain the server system. These data are not to be preserved for the purpose of police investigation. They preserved the data for their purpose. Service providers preserve different data as per their requirement. For example:

3. "Cyber Laws and Appreciation of Electronic Evidence: Challenges", available at: https://www.soolegal.com/roar/cyber-laws-and-appreciation-of-electronic-evidence-challenges (visited on July 15, 2020)
4. Appreciation of electronic evidence, Available at: https://nja.gov.in/Concluded_Programmes/2016-17/P-1007_PPTs/3.%20Appreciation %20of%20Electronic%20Evidence.pdf (Visited on: June 12, 2022)
5. Ibid.

   Internet Service Provider: Internet service providers preserve log details and user details etc.
   Mobile Service Provider: Call details records, customer details records, tower details records etc. are preserved by the mobile service providers.
   Email Service Provider: User details, log details and verified mobile number etc. are preserved by the email service providers.
   Social Media Service Provider: User details & log details etc. are preserved by the social media service providers.
   Digital Payment Service Provider: They also preserve the data of digital payment transaction details[6], user details, beneficiary details, log details and banking details.

Service providers of the Digital Platform are preserves users' data in order to maintain the Company's systems and services. Service providers generally comply with the law of the government under section of the Information Technology Act 2008. Therefore, they provide the data of each user or system to the law enforcement agencies as and when required by law enforcement agencies in their investigations. The data provided by the service provider is used by the investigative agencies to present it as electronic evidence before a court of law. But, questions of integrity and authenticity have always been raised on such electronic evidence (data).

III. Electronic evidence and their admissibility:

Evidence: The apex court has clearly defined appreciation of evidence in *Kajal Sen Vs. State of Assam* that, "The process by which a judge concludes whether or not a fact is proved is called appreciation of evidence. It is a duty of the court to appreciate evidence minutely, carefully, and to analyse it."[7]

Electronic Evidence: Data or information stored or transmitted through electronic means and relating to a crime is considered electronic evidence.

6. Appreciation of electronic evidence, Available at: https://nja.gov.in/Concluded_Programmes/2016-17/P-1007_PPTs/3.%20Appreciation %20of%20Electronic%20Evidence.pdf (Visited on: June 12, 2022)
7. Kajal Sen v.State of Assam AIR 2002 SC617

Electronic evidence means that the "evidence which existed in electronic (intangible) form is being produced in tangible form".[8] Any probative data and information stored or transmitted in electronic form that a party to a court case may use it at trial is called electronic evidence.[9]

Certificate under Section 65B of Indian Evidence Act 1872:

Admissibility of electronic evidence is defined in section 65B(1) of the Indian Evidence Act 1872. According to this section any information contained in an electronic record which is printed, stored, recorded on paper or copied in optical or magnetic media produced by computer shall be deemed to be also a document subject to certain conditions mentioned in section 65B(2).

Electronic evidence must necessarily satisfy the following conditions:[10]
1. It must be produced by a computer that is regularly used to store or process information for the purposes of any activity carried out in the period that the person has legitimate control over the use of the computer keeps;
2. The information obtained in the electronic record was regularly fed into the computer in the normal sequence of activities.
3. Computer was working properly.
4. The duplicate copy must be a reproduction of the original electronic record.
Therefore, a certificate under 65B is required to ensure integrity, authenticity and admissibility of the electronic record.

8. Appreciation of electronic evidence, Available at: https://nja.gov.in/Concluded_Programmes/2016-17/P-1007_PPTs/3.%20Appreciation %20of%20Electronic%20Evidence.pdf (Visited on: June 12, 2022)
9. Eoghan Casey, Susan W. Brenner, et.al.(eds), Digital Evidence and Computer Crime 03 (Elsevier Inc, USA, 2011)
10. Pawan Kumar Shrivastva, "Electronic Evidence in Crime Investigation - Darknet & Policing" 68 The Indian Police Journal 43-51 (2021)

IV. Current Practice and Procedure for Collecting Electronic Evidence (data):
For collecting electronic evidence (data) from various service providers, law enforcement agencies follow their own standard operating procedures. The whole process is conducted in the following steps:

a. Request of Law Enforcement Agencies:
Generally, system administrators of law enforcement agencies or investigation teams communicate through email to the State Nodal Officer of the service provider and request to provide the data under Section 91 CrPC.

b. Nodal Officer:
Each of the service providers has appointed nodal officers to deal with, communicate and assist law enforcement agencies in their investigations. Generally, Indian service providers are appointed nodal officers in each state of India. The State Nodal Officer, under the provision of various sections of the Information Technology Act 2008, forwards the requests of law enforcement agencies to the data centers own system administration.

c. Data Centre:
Data center administrators generate the required data from the service providers' server. The system generated data will be returned back to the state nodal and they forward to the law enforcement agencies.

d. Law enforcement Agencies:
The law enforcement agencies take a print out of the data provided by the nodal officer of the service provider. Agencies submit the print out (electronic evidence) of the data along with the certificate under Section 65B of the Indian Evidence Act-1872 before the court. The System Administrator of the District Police Headquarters issues Certificate 65B of the Indian Evidence Act 1872.
In this scenario, the data is generated and processed in different stages and it has been carry and forwarded many times and by multiple authorities. Therefore, the question of integrity and authenticity of data continues to arise before the court, as the certificate of Section 65B of the Indian Evidence Act 1872 loses its relevance in this multi-layered data processing. In practice, the system administrators at each district police headquarters issue the certificate, while they do not generate the data. And, this is the reason, such electronic evidence does not get due appreciation before the court and at times the benefit of doubt goes to the suspect.

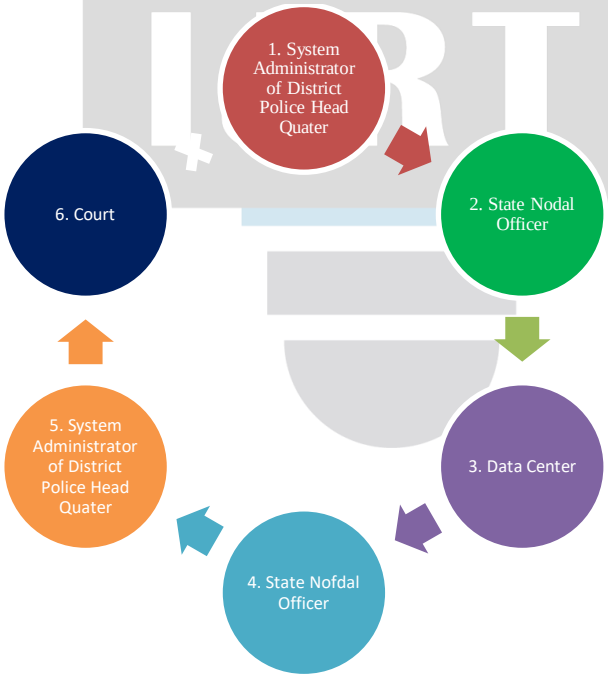

Fig 1: Different stage of Data Processing and Presenting before the Court

V. Empirical Study:

The researcher has conducted an empirical survey to know the working process of collecting electronic evidence from various service providers of the digital platform as well as from police and judicial officers. The researcher has decided to conduct an empirical survey by interview method. Therefore, it has divided the respondents into three target groups; e.g: 1. Judicial Officers, Prosecutors and Lawyers 2. Higher Rank Officers of Police 3. Nodal Officers of Service Providers.In their empirical survey, 17 respondents including 05 Judicial Officers, 03 Prosecutors, 01 Lawyer, 04 IPS (Indian Police Service) officers, 02 Police Inspectors and 02 Nodal Officers of service providers have participated.The researcher wanted to know how many stakeholders and custodians of digital evidence believe that the digital evidence provided by the service provider is highly appreciated by the court. About 95 percent of respondents answered "yes" and believed that digital evidence before court is highly appreciated. In another question, 90 per cent of judicial officers are of the view that the standard operating procedure is not followed by the investigating agencies in their collection and admission before the court. Approx 85 percent of the 15 respondents believe that there are multiple authorities involved in the generation, processing and presentation of the data before the court. During interviews of police officers and nodal officers of service provider, the researcher found that some service providers are already providing limited access to their servers to collect data. Many social media service providers are already providing a dedicated online portal for law enforcement agencies. Through this online portal, the law enforcement agents are directly communicating and making requests to the service providers. Service providers upload their data on this portal and law enforcement agents collect the data (electronic evidence) from this portal. Facebook, Instagram and WhatsApp are some examples of social media service providers that are providing such facilities. Even, many mobile service providers are also providing limited access to certain data on their servers. For example, Airtel and Jio mobile service providers are offering such features.

About 95 per cent of judicial and police officers believe that if all service providers provide customized access to the server (meaning, required in police investigations), the integrity and authenticity of the data will not be questioned as the investigating agencies directly access the data from the server and present it before the court along with the certificate under section 65B of the Indian Evidence Act 1872. However, when the same question was raised by the researcher to the service providers as to why the law enforcement agencies should not be given limited but direct access to the server for certain data, they started making excuses for financial & privacy issues and misuse of customer data.

VI. Conclusion:

Customer data preservation by service providers is a common occurrence in the service provider industries for various purposes. These data are very relevant and play an important role in prosecution. Therefore, law enforcement agencies request service providers for these data (electronic evidence). From the stage of requesting the data and the presentation of data before the court, there are many authorities involved. Due to which, the question of integrity and authenticity of data has always been raised before the court. In cases where data is carried and forwarded at multiple levels, while most of these people do not generate the data, it becomes difficult to determine who will issue the certificate under Section 65B of the Indian Evidence Act 1872. In practice, the certificate is issued by the system administrators at the District Police Headquarters, which is generally not admissible before the courts, as the data is not generated by them. If a certain access to the servers of the service providers is given to the District Police Headquarters, the system administrators themselves will be able to take data from the server and also issue 65B certificates. Then there will be no question on the integrity and authenticity of the data. So far some service providers have provided access to certain data from the server. Who just needs to upgrade and customize these features. So that law enforcement agencies can get the data of their meaning. With such access to the data center servers of the service providers, the involvement of multiple authorities would be eliminated, thereby eliminating questions like data manipulation; and the certificate issued by the system administrator of the District Police Headquarters would be easily admissible before the court. It is also economical and beneficial for the service providers as they will not need to appoint nodal officers on a large scale for each district headquarter.

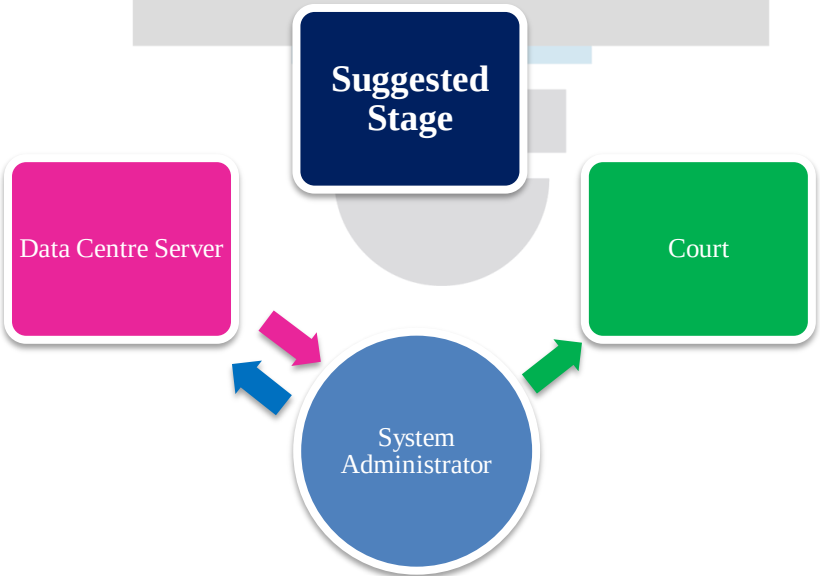

Fig 2: Suggested stage for data collection and their admissibility before the court

Suggestion:

1. The government should enact a law to compel all service providers to provide dedicated online portals for law enforcement agencies.
2. Service providers that provide limited access to their servers may upgrade systems to provide customized but direct access to server data.
3. Service providers who still do not have a dedicated online portal for law enforcement agencies should set up their own systems to provide such facilities.
4. The police department should take appropriate steps from the service providers to address their data security concerns.

REFERENCES:

1. (2012) 9 SCC 1
2. (2010) 4 SCC 329
3. "Cyber Laws and Appreciation of Electronic Evidence: Challenges", available at: https://www.soolegal.com/roar/cyber-laws-and-appreciation-of-electronic-evidence-challenges (visited on July 15, 2020)
4. Appreciation of electronic evidence, Available at: https://nja.gov.in/Concluded_Programmes/2016-17/P-1007_PPTs/3.%20Appreciation %20of%20Electronic%20Evidence.pdf (Visited on: June 12, 2022)
5. Appreciation of electronic evidence, Available at: https://nja.gov.in/Concluded_Programmes/2016-17/P-1007_PPTs/3.%20Appreciation %20of%20Electronic%20Evidence.pdf (Visited on: June 12, 2022)
6. Kajal Sen v.State of Assam AIR 2002 SC617
7. Appreciation of electronic evidence, Available at: https://nja.gov.in/Concluded_Programmes/2016-17/P-1007_PPTs/3.%20Appreciation %20of%20Electronic%20Evidence.pdf (Visited on: June 12, 2022)
8. Eoghan Casey, Susan W. Brenner, et.al.(eds), Digital Evidence and Computer Crime 03 (Elsevier Inc, USA, 2011)
9. Pawan Kumar Shrivastva, "Electronic Evidence in Crime Investigation - Darknet & Policing" 68 The Indian Police Journal 43-51 (2021)