Legal Challenges and Cyber Crimes Faced in Times of Huge Data and DiverseStorage Systems

Dr. Rishikesh Singh Faujdar[*]
Mr. Amit Tyagi[**]

Abstract

Over the last 20 years the storage devices in the cyber world have changed its shape and capacity. The storage devices have increasingly turned smaller in size, while the storage capacity is increasing. Even as we look back in the last two decades the storage capacity of devices has changed in a big way. At the start of the century, floppy disks were considered for storage of data as well as transferring data from one computer system to another computer system. With the passage of time floppy disks became outdated and their place was taken over by compact disks commonly known as CD. There was a huge difference in the storage capacity of floppy disks vis-a-vis CDs. People were able to store much more data on the CD drive as compared to floppy disks. Towards the start of last decade CDs started becoming obsolete, so much so that the new laptops do not even support CD Drive. Hard drives and pen drives came into existence. These drives also saw a transformation where in initially they were much bulkier as compared to what is being produced in the current times. External hard drives became much more popular as they would store many GB of data at one location and they were easy to move around from one place to another.

As we entered into the current decade, we saw that the data that is being generated across the world is much more than what was generated 20 years back. The number of people who are using devices has increased in terms of millions. The number of people who are using the internet has also increased many times. The types of devices have also changed. Mobile phones brought in a revolution in the storage of data as well. Earlier the data stored in the mobile phones was only related to some message or some small files. With every new generation of mobile phones coming in the market the capacity of storage has also increased. As the world looks at such a huge amount of data the world is also trying to solve the problem of storage of this data. Another challenge that is being solved is the transfer of data from one person to another or from one source to another. This is where

[*] Assistant Professor, School of Law, Sharda University, Greater Noida, U.P
[**] LL.M Scholar, Sharda University, Greater Noida, U.P

the cloud systems. Cloud is nothing but a shared storage system where data from multiple people can be stored at big servers which can accommodate millions of data records. People are putting up data in the cloud. It gives the advantage that the data can be stored at a central location without being worried about deleting data accidentally.

The smaller storage devices have also presented a challenge for law enforcement agencies in solving cyber related crimes. In the earlier times it was much easier to retrieve data from a computer hard disc and use it as evidence.

This paper talks about the issues and challenges faced by the law enforcement agencies in investigating the crimes in the times of increasing data and the diverse storage devices, particularly when crimes are committed in the cyber world.

1. HISTORY OF DATA STORAGE DEVICES

It was the first attempt at creating a data storage device. Holes in a punching card stored a sequence of instructions which were used to communicate with different types of equipment. Some of the equipment in which punching cards were used includes a piano and textile looms. Punch cards found a lot of their usage in the second half of the 20th century.

In the 1960s, "magnetic storage" gradually replaced punch cards as the primary means for data storage. In 1965, Mohawk Data Sciences offered a magnetic tape encoder, which was dubbed as a replacement for punching cards. In 1990, the combination of personal computers and magnetic disk storages became popular and punching cards made their way out of the system[1].

In the past data storage and memory were the two words which were used interchangeably. Now data storage is the superset which includes memory. Memory is more of a short-term while data storage is considered forever.

IBM is primarily responsible for driving the early evolution of magnetic disk storage[2]. They invented both the floppy disk drive and the hard disk drive and their staff are credited with many of the improvements supporting the products. A floppy disk was a removable device with very less storage but was easy to use. It had a magnetic film and was pretty inexpensive to make. The flip side was that it was easy to damage as well.

[1] https://www.dataversity.net/brief-history-data-storage/ (Visited on 28-Jun-2021)
[2] https://www.ibm.com/ibm/history/exhibits/storage/storage_chrono20.html (Visited on 27-Jun-2021)

Floppy disks were soon replaced by compact discs. These used light as a medium to record. James T. Russel[3] invented these and it led to CDs (Compact Discs) and DVDs (Digital Video Recordings) and Blu-Ray. (The word "disk" is used for magnetic recordings, while "disc" is used for optical recordings. The storage capacity of these devices increased manifold and were used about the early part of the 21st century.

Flash drives appeared on the market, late in the year 2000[4]. A flash drive plugs into computers with a built-in USB plug, making it a small, easily removable, very portable storage device. Unlike a traditional hard drive, or an optical drive, it has no moving parts, but instead combines chips and transistors for maximum functionality. Generally, a flash drive's storage capacity ranges from 8 to 64 GB. (Other sizes are available, but can be difficult to find.)

The word moved into the 21st century and a new type of storage device came into existence, these are called flash drives. A flash drive could be plugged into a computer system which would already have a USB plug-in option. This made it very easy to plug in, remove and transfer from one system to another.

Advantage with the flash drive is that it can be rewritten any number of times[5]. These drives have capacities and can Store GB of data. This is the reason that Floppy disks and CDs are now out of the market. Flash drives are also named as pen drives, USB drives or solid state drives.

2. INTERNET USAGE AND INCREASE IN DATA STORAGE DEMAND

Across the world, the internet is growing at a fast pace. In 2019, the number of users using the internet across the globe was 3.97 billion[6], which means that more than half of the Global population is currently connected through the internet. As more and more people continue to get connected to each other, they also generate a lot of data which needs to be stored in a manner that is easily accessible and maintainable.

It is said that data is the new oil. It means that data will have the same value as the value of oil. What is the volume of data that we anticipate will be generated in future? This is a question which needs to be answered so that the future data storage needs can be

[3] "Inventor of the Week - James T. Russell - The Compact Disc" (Visited on 27-Jun-2021)

[4] Harris, David; Harris, Sarah (2010). *Digital Design and Computer Architecture*. Morgan Kaufmann. pp. 263–4

[5] https://www.datadirectinc.com/blog/15-Ways-Why-Flash-Drive-is-a-Better-Recordable-Media-Device-than-Blu-Ray.html (Visited 26-Jun-2021)

accomplished. According to projections from Statista, 74 zettabytes of data will be created in 2021.In the year 2020, 59 zettabytes of data was generated while in the year 2019, 41 zettabytes of data was generated[7]. If you look at this trend, the word is adding close to 15 zettabyte of more data every year.

The growth of data is not going to slow down. In fact the data protection is set to continue and is going to accelerate in future.

Following are some of the reasons that are increasing the growth of data:-

- Cloud computing
- Ever improving consumer electronics
- Ever increasing presence of people on social media
- Easy access of Smartphones which support various types of video filming
- Large development in field of new technologies
- Increase the usage of applications in daily life
- Introduction of machine learning and artificial intelligence

3. CHALLENGES FACED IN RELATED TO DATA AND DATA STORAGE[8]

As the data is increasing the word is also facing some challenges in managing this data. Some of the challenges are mentioned below: -

- **Security of data** - The increase in data is also creating a bigger problem of handling such a huge amount of data safely. As per an estimate an average data breach cost about $3.86 million[9]. With the increase of that, it is important to secure the data from both internal and external threats.

- **Quality of data** - The increase in data has also created a big problem of quality of data, such as which cannot help in providing any inference or information. It will be the focus that the data pipelines should be automated and the data is kept clean when it enters anyone's system.

[7] https://www.cloverdx.com/blog/how-much-data-will-the-world-produce-in-2021 (Visited 28-Jun-2021)
[8] Agrawal, Rajeev & Nyamful, Christopher. (2016). Challenges of big data storage and management. Global Journal of Information Technology. 6. 10.18844/gjit. v6i1.383.
[9] https://www.ibm.com/security/data-breach (Visited on 29-Jun-2021)

- **Standardizing the data** - In order to and show so that everyone who is handling the data is on the same page and in order to enable collaboration among different teams and people accessing the data across the word it is important to use data modelling and standardise the storage of data, maintenance of data, transfer of data and manipulation of data.

- **Focusing on compliance** - There are many regulations which are very stringent and strict to follow. All the different countries have different ways of regulating the data. It is another challenge that is faced by the people who are involved in storage, maintenance and security of data.

4. CYBER CRIMES AND CYBER LAWS

It is said that a crime can take place only when there is a chance for a suitable target for the same, when the people who are supposed to protect the target are not capable and where the perpetrator of the crime is really sure of when to commit the crime[10].

More and more people are working on the internet. As people have started using the internet for various tasks, the criminals have also started using the internet for committing crimes. Cyber-crimes are nothing but crimes of the real world perpetuated in the medium of computers and hence there is no difference in defining a crime in the cyber world and real-world. Only the medium of crime is different.

Though many people have tried to define cybercrimes, the Council of Europe[11] adopted its convention on cybercrime Treaty known as Budapest convention which has identified different activities as Cybercrimes. Some of the important activities are: -

- Intentional access of a computer system without proper right
- Intentional interception of non-public transmission of computer data
- Intentional damage, deletion, alteration for separation of computer data
- Intentional and serious hindrance in the functioning of a computer system by damaging or suppressing the computer data
- Production, sale, procurement or usage of similar data with intent of committing a crime

[10] Talat Fatima, *Cyber Crimes* (Eastern Book Company, New Delhi, 2016)
[11] https://www.coe.int/en/web/cybercrime/the-budapest-convention (Visited 24-Jun-2021)

It is important to find out ways of convicting a cyber-criminal. If the conviction does not take place, there remains a threat to a person's reputation, the privacy of an individual which is against the right to privacy, to the data, which can harm the interest of an individual, to the financial transactions of the victim. The low conviction emboldens the criminal and they end up using the cyber methods in doing traditional crimes, in acts of terrorism and in financial scams which involve the movement of money in an unlawful manner. One of the issues that agencies face is the enforcing of cyber laws. As climate does not have a boundary, cyber world also is borderless. The law that governs the cyber world is different in different countries. A very different way of solving this problem of different laws in different countries is to come up with cyber laws which are applicable across the world. Though this thought is very radical but in order to tackle the increasing cyber-crimes and ensuring that criminals do not take the territorial advantage, this is worth considering.

As most cybercrimes are transnational in character, inconsistency of laws and regulations across country borders makes it especially difficult for countries to cooperate when investigating cross-border cyber-crimes. When a cybercrime takes place, a big problem faced is the jurisdiction[12]. In cases where origin of the crime is one jurisdiction while the target of crime is in another jurisdiction. Some of the other issues are related to privacy concerns, protection of data, issues related to IP, increase of cyber-crimes across the globe, potential increase of terrorism using cyber world, issues related to the pornography, particularly related to children. Countries are facing major challenges in tacking these cyber-crimes.

5. CYBER CRIMINALS AND FOCUS OF DIGITAL FORENSICS

First of all we need to understand the difference between forensics and anti-forensics. While the term forensics is quite specific and clear it is difficult to define the term anti-forensics. Anti-forensics can be understood as a set of tools, methods and various processes that are applied in order to avoid any such analysis that is important from an

[12] *Challenges to enforcement of cyber-crimes laws and policy*, By Ajayi, E. F. G. in the Journal, "Journal of Internet and Information Systems" Vol. 6(1), pp. 1-12, August 2016

evidence point of view in the court[13]. Different anti-forensics methods are employed by criminals[14]:

- **Hiding of data** - Tools can be used to hide the data. Data can be stored and manners which are difficult to figure out or in ways which are not easily accessible
- **Artefact Wiping** - There are different software's available for recovering the storage space on a computer system. This software is used for illegitimate purposes. Criminals also used such software's like evidence eliminator; secure clean and window washer to remove search data which can act as evidence[15].
- **Clearing the trail** - Different methods have been used in order to confuse the investigators. Email anonymizers or Web anonymizers ostensibly provide privacy services which prevent an investigator from finding out the source from where the crime has originated. Service logs are system event items files are deleted in order to clear the trail of any criminal activity.

Let us look at the focus areas for the cyber investigating agencies and cyber forensics team, particularly against the cyber-crimes which involve data and data storage[16].

- **Large volume and High Speed** - The investigating agencies have faced a lot of issues in storing, accessing and processing large amounts of data for forensic purposes. The volume of data which is due to the multimedia rich contents is a challenge for the investigating agencies in collecting clues and detecting infringements. This problem is compounded in the case of data which is transported from one system to another because capturing and storing the necessary information of data traffic is a huge task.
- **Complexity of the storage systems** - The increase in data has also resulted in coming up with innovative methods of storing the data. The Stored data is not

[13] Garfinkel, Simson. (2007). Anti-forensics: Techniques, detection and countermeasures. 2nd International Conference on i-Warfare and Security.
[14] Chhabra, Gurpal. (2014). Anti-Forensics Techniques: An Analytical Review. 10.1109/IC3.2014.6897209.
[15] https://info-savvy.com/anti-forensics-techniques-trail-obfuscation-artifact-wiping-encryption-encrypted-network-protocols-and-program-packers/ (Visited on 27-Jun-2021)
[16] https://www.computer.org/publications/tech-news/research/digital-forensics-security-challenges-cybercrime (Visited on 27-Jun-2021)

confined to just one single location, but it is now distributed among multiple physical or virtual locations such as service across the globe, on cloud, on social media networks and where there are other networks which are attached to the storage units. This becomes a challenge for reconstructing any evidence in a complete and correct manner because there is a depth of expertise and tools to do the same. Another challenge is the pace at which the data can be deciphered. Since the system has become more Complex it is difficult for forensic teams to convert the data in meaningful evidence.

- **Lack of standards -** There are a lot of technological advancements that have taken place over a period of time. Still files are the most popular digital artefacts to be collected, categorised and analysed. Researchers have tried to come up with some standards around data but haven't met with a lot of success. Lack of collaboration among various parties create a lot of problems for foreign six and investigation teams in understanding and deciphering the data stored in case of cutting-edge Cyber-crimes.
- **Securing the privacy of individuals -**The advancements in social media and online social networks has made personal information of people more vulnerable. We have seen multiple instances of Identity theft or identity fraud that have been committed after getting access to personal details of individuals who are on various social networks. It is a huge problem for forensics and investigating Agencies to collect information in order to locate the origin of an attack which can violate the privacy of individuals.
- **Anti – forensic methods** - There are many different methods of securing the data. For example, encryption of data, obfuscation of data etc. In order to create an airtight case for Cyber-crime collecting evidence is essential. To achieve the same, people investigating crime need to have the best tools available. There is a need to create new methods and new forensic tools which can help in tracking cyber-crime cases.

6. LEGAL CHALLENGES FOR FORENSIC TEAMS

Apart from different types of technical challenges faced by investigating agencies there are some legal challenges as well which digital forensic teams have to encounter[17].

- **Admissibility of evidence -** One of the biggest challenges is to ensure that the evidence that is being presented will be considered as admissible evidence.
- **Absence of guidelines and standards-**In India, there are no proper guidelines for the collection and acquisition of digital evidence. The investigating agencies and forensic laboratories are working on the guidelines of their own. Due to this, the potential of digital evidence has been destroyed.
- **Privacy issues** - The introduction of privacy legislation has created uncertainty in digital forensic about what is permissible behaviour in collecting and retrieving personal informant. These privacy provisions have not been adequately tested in the court to provide a comprehensive common law background.
- **Preserving the electronic records** -In the case where the electronic evidences could be admissible, an issue which is addresses the preservation guidelines uncovers the fact that preserving an electronic evidence, which may involve a technical process, is itself a challenge as there are instances where a case law lived up for more than 20 years. Preserving an electronic evidence for more than 20 years is not possible as within that period the technology may evolve many folds. The preservation of electronic evidence for a long time takes a lot of money and technology.

7. CONCLUSION AND WAY AHEAD

The world is becoming more interconnected and is generating large volumes of data. As people move from physical activities to digital activities; cyber criminals are also using the internet and digital devices to commit different types of crimes. These crimes are resulting in loss of a person's reputation, money and can also be a threat to his life. In order to investigate these types of crimes it is important that the investigating Agencies are ahead of the criminals. The field of digital forensics has to keep pace with the activities and innovations shown by criminals in the cyber world. It is all the more important due to the

[17] https://legaldesire.com/challenges-faced-by-digital-forensics/ (Visiting 29-Jun-2021)

emergence of new trends like Crime as a Service (CaaS)[18], which lets anybody execute serious cybercrimes. Hence it is important that the new forensic tools that are being produced should support different types of investigations, ensure that there is privacy of the victim as well as people who are involved in investigation and are easily scalable so that the investigating Agencies and forensic teams are always ahead of the criminal.

*****

[18] https://www.stickman.com.au/cyber-security-blog/what-you-need-to-know-about-crime-as-a-service-caas/ (Visited on 29-Jun-2021)