Symbiosis Law School, Nagpur Multidisciplinary Law Review
Volume II Issue II (2023), ISSN: 2583-1984 (Online), Pg. Nos. 186-195

SCOPE OF CYBER EVIDENCE WITH SPECIAL REFERENCE TO SMART DEVICES

Malvika Mahajan*

ABSTRACT

Witness testimonies till date serve as the primary tool for establishing an account of the events as well as a tool for assisting in establishing the truth of the matter. However, an inevitable consequence of witness testimonies is the emotional aspect of the testimony as well as the subjective analysis, which is as good as a researcher's bias in a study of independent variables. While pondering on the solution for removing such areas of subjectivity, one often finds its way back to technology. The current literature focuses on technology hampering job security, and its implications on policy making, it begs the question, how does it impact the courtroom? Moreover, while studies have focused on the utilization of digital evidence, the literature often focuses on digital evidence used to corroborate crimes in the digital sphere, for instance, hacking, identity theft, or child pornography. However, digital evidence is slowly being introduced in the judicial system to corroborate the determination of bail applications, such as in the recent case of "Drugs on Cruise" involving Aryan Khan. Thus, the paper aims at analysing the usage of digital evidence in corroborating crimes of a physical nature, and the scope of its admissibility in a court. Furthermore, it analyses the persuasiveness of digital evidence vis-à-vis witness testimonies.

Keywords: *digital evidence; smart devices; evidentiary value; witness testimonies*

* NMIMS Kirit P. Mehta School of Law, Email: malvika1249@gmail.com.

SCOPE OF CYBER EVIDENCE WITH SPECIAL REFERENCE TO SMART DEVICES

Introduction

The Hon'ble Court in the Suresh Kalani case[1] highlighted the notable fact that a presumption can only be drawn from facts, and cannot be drawn from other presumptions, i.e., the same follows logical reasoning, whose deductions are primarily based on the facts. This sheds light on the importance of the type of evidence, especially circumstantial evidence and the evidentiary value attached to such evidence. Digital evidence refers to any information obtained from the Internet of Things [IoT] and surveillance cameras. The evidentiary value of digital evidence is not explicitly provided for in the Indian Evidence Act, however, its provisions can be interpreted to encompass such evidence.

General Definitions

Primary Evidence

Sec. 62 of the Indian Evidence Act defines primary evidence to mean documents itself produced for the inspection of the Court, which includes but is not limited to printouts, photographs, lithography, etc.

Secondary Evidence

Sec. 63 of the Indian Evidence Act defines secondary evidence to include certified copies, oral account of an original document by the person who has viewed the original document, and mechanical copies including the counterparts of a particular document. The procedure with respect to obtaining certified copies has been provided for under Sec. 65B of the Indian Evidence Act.

[1] State of Maharashtra & Anr. v. Pappu alias Suresh Budharmal Kalani, (2014) 11 SCC 244).

Electronic Record / Data

Sec. 2(1)(t) of the Information Technology Act defines electronic record to mean any data, image or sound received, stored, or sent in an electronic form.

Legislation Involved

- Sec. 2(1)(t) of the Information Technology Act, 2000 defines electronic record.
- Sec. 65B of the Indian Evidence Act, 1872 categorises electronic records as admissible documents in a court of law.

Discussion

Case 1 – Data Recorded by Fitbit Watches

Myrna Nilsson – Supreme Court of Australia

Facts of the Case: In September 2016, a lady called the police on watching her neighbour emerge from her own house with her hands tied and mouth bound. On being questioned by the police, the neighbour narrated the incident that translated through the night leading to the death of her 57-year-old mother-in-law. As per the neighbour, Caroline Nilsson, her mother-in-law Myrna Nilsson, the deceased was followed home by a group of men, who she argued with for 20 mins outside their house. The men gave a fatal blow to her head; however, this attack was not heard by the daughter who was in the kitchen with the door locked. Subsequently, they bound Caroline's mouth with tape and tied her hands before fleeing the scene.

Use of Digital Evidence: Myrna Nilsson, the deceased wore a Fitbit watch which recorded her breathing, footsteps, as well as heartbeat on a daily basis. On the night of the murder, the Fitbit recorded a normal breathing followed by a state of shock and heavy breathing. This led the police to determine the time of attack when the deceased would have lost consciousness which corresponded with the state of unlevelled breathing to be 6:38 P.M. and the death of

the deceased was conclusively determined to be 6:40 P.M. However, the neighbour saw and immediately called the police at 10:10 P.M. which as per the narration of Caroline happened moments after her being bound. The discrepancy of 3 hours in the facts narrated, and the evidence retrieved lead the police to believe that the murder of Myrna was staged by Caroline, who utilised the 3 hours to discard of all bloodied clothing, and further rid the laundry room of any evidence[2]. Caroline is thus convicted by the jury on the charge of manslaughter.

Case 2 – Data Recorded by Amazon Echo

Adam Reechard Crespo – Florida Case

Mechanism of Amazon Echo: The device of Amazon Echo has been recognised to respond to any questions or queries of the users in response to a word of activation which usually includes the word Alexa, however, the users may opt for any activation phrase. On the mention of the activation phrase, every command or question that follows is recorded in the cloud server of Amazon, to aid the echo device to function smoothly to respond to such queries or recognise spoke triggers for a future date. The options with respect to hard mute or change of voice triggers can only be effectuated through the Amazon app[3].

Facts and Progress of the Case: Adam Crespo was charged in 2019 for the murder of his wife Silvia Crespo who was found dead in the apartment with a spear wound. However, on being questioned, Adam stated that the wife entered the room and in the course of the agreement, Adam got hold of the spear which was against the bed, and it snapped as a result of an accident. Since the parties had an Echo Dot in the room, and the Echo Dot had a different wake word as compared to Alexa, thus, the police are hopeful that the Echo Dot got activated

[2] Parmeny Olson, Fitbit Data claim in Courtroom, Forbes (Sep. 29, 2022, 10:59 PM), https://www.forbes.com/sites/parmenyolson/2014/118/16/fitbit-data-use-court-room-injury-claim/?sh=541063873790.

[3] Anjelica Cappellino, Amazon Echo: Expert Witness in a Murder Trial? Expert Institute (Sep. 29, 2022, 11:05 PM), https://www.expertinstitute.com/resources/insights/amazon-echo-expert-witness-murder-trial/.

during the course of the agreement and recorded any instance of foul play inside the house. Thus, the police filed for a warrant for gathering the Amazon Echo Dot recordings, however, Amazon refused to provide client information unless the same is required by a legally binding and valid order.[4]

Case 3 – WhatsApp Messages

A2Z Infraservices Ltd. v. Quippo Infrastructure Ltd., 2021

Facts of the Case: South Delhi Municipal Corporation entered into an agreement with A2Z Infraservices for the collection and transportation of certain items of waste. Infraservices further contracted with Quippo Infrastructure to decentralize its responsibilities and to undertake a part of the contract. The agreement specifically provided for the deposit of all money into an escrow account which would be utilised to make payments to appropriate parties entering into sub-contracting agreements.

Judgement of the Calcutta High Court: On 28 May 2020, A2Z Infraservices terminated its contract with Quippo, who moved to the Calcutta High Court. The Court relied on whatsapp messages in which A2Z made an unequivocal admission to receiving a payment of 8.8 Crore. Furthermore, Quippo relied on an email to verify the agreement to deposit all fees received not an escrow account. A2Z Infraservices moved to the Supreme Court on the contention that the WhatsApp messages were fabricated by Quippo.

Judgement of the Supreme Court: The Supreme Court did not pronounce a ratio with respect to the admissibility of WhatsApp messages, however, they refused to rely on WhatsApp messages as evidence of the business agreement[5] by stating that, "Anything can be fabricated

[4] Kayla Epstein, Amazon to have information in Stabbing Case claims Police, Washington Post (Sep. 30, 2022, 4:56 PM), https://www.washington-post.com/technology/2019/11/02/police-think-amazons-alexa-to-have-information-stabbing-case/.

[5] Anu Bhuvanachandran & Ajay Kumar Jha, Evidentiary Value of Whatsapp Messages, The Daily Guardian (Sep. 29, 2022, 6:15 PM), https://thedailyguardian.com/the-evidentiary-value-whatsapp-messages-india%EF%BB/.

today related to social media; hence, we don't attach any evidentiary value to the messages on WhatsApp."

Prior to the 2021 judgement, the Court in Arjun Panditrao Khotkar v. Kailash Kushanrao[6], laid down certain exceptions to the requirements laid down in Sec. 65B with respect to WhatsApp messages as digital evidence. WhatsApp messages were recognised as secondary evidence, which required a certificate under Sec. 65B of the Evidence Act, however, the Court stated that reproduction of the very device which contains the WhatsApp messages would be considered as primary evidence in a court of law. Furthermore, cases where the original device is not in possession with the owner, then the production of a certificate under Sec. 65B would be rendered useless preventing the parties from producing any information even as a secondary piece of evidence. Thus, the Court recognised the impeding conditions as an exception to the mandatory requirement as provided in Sec. 65B of Evidence Act.

Analysis

Advantages

- In Myrna Nilsson's case, the time of death would have been solely determined through forensic experts who would have narrowed the time to a larger window of hours, allowing for Caroline Nilsson's story to stand.
- Adducing a timeline of events also requires testimonies of several witnesses, the lack of which raises question on witness credibility where the victim is the sole witness in cases where the crime occurs inside the house or in a private space. Therefore, the absence of witnesses does not hamper the process of justice, with the introduction of digital gadgets and software that record every movement and breath of an individual.
- The right of privacy of an individual is not absolute as pronounced by the 9-judge bench in the Puttaswamy judgement[7]. Moreover, the right, though being a

[6] Arjun Panditrao Khotkar v. Kailash Kushanrao, (2020) 7 SCC 1.
[7] Justice K. S. Puttaswamy (Retd) & Anr. v. Union of India, (2017) 10 SCC 1.

fundamental right, can be curtailed through the due process of law, which in India is recognised under the Code of Criminal Procedure. Furthermore, the right can be curtailed in the interest of justice under the well-established 'principle of greater good'.

Disadvantages

- When we look at WhatsApp chats or social media posts, in majority instances it can aid in understanding the intent of the person but cannot be proof of the commission of an act. Even if the WhatsApp communication is of an admission or confession by a person, the same would be categorised as an extra-judicial confession. It has been well established that extra-judicial confessions hold no or little value in evidence, and the same cannot be given any weightage unless it is made in front of a magistrate.
- The privacy policy of several gadgets and smart audio assistants such as Alexa, clearly state the non-recording or storage of any data of the users, for instance, the system of end-to-end encryption promised to WhatsApp users. For instance, Amazon may refuse to share the data recorded as seen in the case of the San Bernardino shooter, where Apple refused to break into the device of the shooter to provide the FBI with information. As illegally obtained evidence is admissible in a court of law in India, the defence attorneys, on refusal by the owner, would hire third-party agents to retrieve such recorded data8.
- All digital evidence may not be recoverable through one device such as a Fitbit watch, but may involve social media platforms, emails and Fitbit information. Combing through such massive logs of data available and stored on smartwatches and other connected home devices would increase the time undertaken for a trial and would further not be suitable in cases that do not represent high-profile cases such as major homicides.

[8] Antara Jha, Cybercrime and Digital Evidence, Financial Express (Sep. 30, 2022, 2:27 PM), https://www.financialexpress.com/defence/cybercrime-and-digital-evidence/2632164/.

- Owners of such smartwatches and TVs may also refuse the very act of storage and recording of pertinent data that the company stores and utilises for better SEO, recommendations to the users, or to track the highest usage of a particular emoji.

Suggestions

- After 300 prisoners escaped from manual monitoring of the police officers on 10th September, 2020, the Supreme Court expressly stated that the law enforcement must advance towards technological advancements. Thus, the current pandemic saw the shift in judicial opinions from placing heavy emphasis on the right to privacy to the usage of technology in the interest of society. Various states released the prisoners under mandatory surveillance and the police officials were allowed domiciliary visits and using monitors and bracelets to track the prisoner's movements. The court has expressly held that in matters of public interest, an exception can be drawn to the rights of the accused and the use of technology must be permitted[9].
- While elaborating on this decision, the Court observed, that a released convict cannot have the same expectation of privacy as that of a citizen and thus, cannot expect the same protection to be guaranteed to the citizens under the constitution. However, accused can and have the same expectation of privacy as that of other individuals, as well as the victims, thus, the disclosure of all contents, such as WhatsApp messages, emails, spreadsheets, or even Fitbit data should not be a presumption, that is, the disclosure of all such material should not be mandatory at the time of filing a suit, or defence, but must be disclosed in court after proving its relevance to the matter, and after reasonably proving that an inspection of such material would reveal relevant information regarding the contention as well as innocence of a party. Thus, for effectuating the above-mentioned point, the investigators must limit the search to specific conversations.

[9] Selvi v. State of Karnataka, 2010 (7) SCC 263 (2010).

- In the first instance attempt must be made to review the material remotely without the need for production of the devices of the parties. In the absence of this, a time limit must be fixed by the Court for reviewing the material without unnecessary delay.
- Information that is irrelevant, especially after the lapse of the trial must be redacted by the investigators, and the use of such information must be limited to the proceedings without any authority for third party publication.

  The complainant or witness whose device in under review must be informed of the procedure, timeline and rights with respect to collection, storage and disclosure of information gathered.
- On refusal of granting information through such digital devices, the Courts may stay the proceedings, or even cancel a specific defence of the person. And thus, to ensure adequacy of the trial, the Court must analyse not the significance of the material to be gathered, but the impact of the absence of such digitally stored material.

Conclusion

The 2005 case of the BTK killer[10] (Bind, Torture, Kill-Strangler) that claimed the lives of 10 individuals, highlights the importance of digital evidence, wherein the serial killer was caught and convicted due to the reliance on a floppy disk[11]. The floppy disk or pen drives, admissible in a court of law[12] have evolved into smart TVs and phones, spreadsheets in a computer, and even the browser history in a computer. In conclusion, a slow progressive approach towards the utilisation of digital records, as opposed to its complete discontinuance due to the issues posed by such use is recommended. Furthermore, the benefits highlighted by use of digital evidence far outweigh the shortcomings of physical evidence as well as witness testimonies and further strengthens the scope of evidence with the introduction of a robust digital mechanism. Nonetheless, the data recorded by the smart devices need to be

[10] Matt Zbrog, Catching the BTK Killer, Forensics Colleges (Sep. 29, 2022, 11:15 PM), https://www.forensicscolleges.com/blog/forensics-casefile-btk-strangler.
[11] National Institute of Justice, Digital Evidences & Forensic, NIJ ((Sep. 30, 2022, 3:30 PM), https://nij.ojp.gov/digital-evidence-and-forensics.
[12] Indian Evidence Act, 1872, § 63, No. 1, Acts of Parliament, 1872 (India).

corroborated by independent witnesses, as well as, the expert witness as a safeguard to understand the reliability, and functioning of the device, especially with increased chances of tampering by tech-savvy individuals.