Himachal Pradesh National Law University, Shimla (India)

Journal Articles HPNLU Journal of Social Sciences

Volume: I (2024)

Impact of Advanced Digital Forensics on Privacy Law: A US-India Perspective

Prachi Mishra & Ashish Kumar Singhal

This article can be downloaded from:
https://hpnlu.ac.in/journal-level-3.aspx?ref-id=37

ISSN: XXXX-XXXX

Recommended Citation:

Prachi Mishra & Ashish Kumar Singhal, *Impact of Advanced Digital Forensics on Privacy Law: A US-India Perspective*, I HPNLU JSS. 206 (2024).

IMPACT OF ADVANCED DIGITAL FORENSICS ON PRIVACY LAW:
A US-India Perspective

Prachi Mishra & Ashish Kumar Singhal[1]

Abstract

Digital forensics has become a vital tool for law enforcement authorities in the investigation and prosecution of criminal offenses. However, the use of digital forensics creates significant privacy and civil liberties problems. With the advancement in technology, individuals' personal data, such as web surfing history, social media activity, and communication, has become increasingly exposed for collection and analysis. Individuals' online activities, including with others, can be tracked using digital forensics technologies which implies violation of private rights which may impact the right to a fair trial and due process.

This article highlights the impact of digital forensics on privacy and civil liberties. It further investigates the possible risks and benefits, highlighting concerns over irrelevant data collection and the potential for digital evidences to be tampered or altered. It underscores the fact that digital forensics can complicate the defence's ability to challenge evidence. This paper also suggests measures to address these concerns. This could involve placing policies and procedures in place to restrict the reach of investigations into digital forensics, making sure investigators are properly trained in these techniques, and creating guidelines for digital evidence's admission in court.

Keywords: Digital Forensics, Privacy Rights, Civil Liberties, Criminal Investigations, Defence

[1] Prachi Mishra, Assistant Professor, UPES Dehradun & Research Scholar, ICFAI Law School, The ICFAI University, Dehradun, India,
Dr. Ashish Kumar Singhal, Associate Professor, ICFAI Law School, The ICFAI University, Dehradun, India

Introduction

The field of digital forensics is fast developing, and criminal investigations are using it more and more frequently. Digital forensics refers to the process of accumulating, analyzing, and preserving digital evidence for use in legal proceedings. It entails extracting electronic data from a wide range of devices, including smart phones, desktops, laptops, and tablets, using specialized tools and procedures.[2] This data, which includes information on chats, purchases, and other internet activity, can subsequently be analysed to give evidence in criminal cases. As electronic devices and online communication are increasingly employed in the commission of crimes, digital forensics has become an essential tool in modern criminal investigations.

Although digital forensics can be useful in criminal investigations, it also raises serious concerns about privacy and civil liberties.[3] One of the major concerns is the possibility for digital forensics technologies to gather data that is not relevant to the investigation. When law enforcement agents grab a smart phone as part of an investigation, for example, they may be able to view data other than what is directly linked to the case, such as personal contacts, images, and texts.[4] This can be quite intrusive and may result in privacy violations. Furthermore, digital forensics methods and procedures have the potential to violate individuals' privacy rights by granting law enforcement organizations access to personal information held on electronic devices or online accounts. Furthermore, these techniques can be used to track people's online activities, such as their web surfing history, social media activity, and interactions with others. This amount of surveillance is intrusive and may violate individuals' right to privacy. Another source of concern is the possibility

[2]M. Sadiku, M. Tembely, et. al.,*Digital Forensics* (2017) *available at* - https://www.researchgate.net/publication/318665422_Digital_Forensics. (last visited Sep. 17, 2024).

[3]M. Seyyar and M. Geradts, *Forensic Science International: Digital Investigation. (2020)avaialble at* - https://www.sciencedirect.com/science/article/pii/S2666281720300263. (last visited Sep. 17, 2024).

[4] L. Newman, How Law Enforcement Gets Around Your Smartphone's Encryption (2021) *available at* - https://www.wired.com/story/smartphone-encryption-law-enforcement-tools/. (last visited Sep. 17, 2024).

of digital evidence being changed or misconstrued. Digital data can be manipulated or erased, either purposefully or unintentionally, jeopardizing the evidence integrity. Furthermore, the intricacy of digital forensic investigations raises the possibility of analysis errors and inaccuracies, which could lead to false convictions or other miscarriages of justice.[5]

The use of digital forensics in investigations raises serious concerns regarding the right to a fair trial and due process. Digital evidence may be the only or principal evidence used against an accused person in some circumstances. As previously stated, digital evidence can be difficult to evaluate and may be prone to manipulation or inaccuracy.[6] Furthermore, the introduction of digital evidence might make it difficult for the defence to refute the evidence since they may lack the technological expertise or resources to fully analyze the data[7].

The purpose of this article is to look into the impact of digital forensics on privacy and civil liberties and further aims to add to the current debate about how to effectively combine the need for effective law enforcement with the need to preserve individuals' privacy rights and civil liberties by investigating the potential hazards and benefits of digital forensics in criminal investigations.

Role of Digital Forensics in Criminal Investigation

The field of digital forensics is crucial in contemporary criminal investigations. Due to the proliferation of technology, digital devices have become an indispensable component of our daily existence. Hence, digital devices frequently harbour crucial evidence in criminal inquiries, encompassing emails, chat logs, photographs, videos,

[5] P. Reedy, *The risks for digital evidence. Strategic Leadership in Digital Evidence* (2021) *available at* - https://doi.org/10.1016/b978-0-12-819618-2.00012. (last visited Sep. 18, 2024).

[6] C. Miller,*A survey of prosecutors and investigators using digital evidence: A starting point* (2020) *available at* - https://doi.org/10.1016/j.fsisyn.2022.100296. (last visited Sep. 18, 2024).

[7] C. Karagiannis & K.Vergidis, *Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal* (2021) *available at* - https://doi.org/10.3390/info12050181. (last visited Sep. 18, 2024).

and other forms of digital data. Furthermore, it aids investigators in gathering, examining, and presenting this information as substantiating evidence during legal proceedings.[8]

Digital forensics applies to various criminal investigations, encompassing cybercrime, fraud, manslaughter, and terrorism. Within cybercrime investigations, the application of digital forensics can facilitate the identification of the origin of a cyber-attack, trace the perpetrator's actions, and retrieve stolen data.[9] Digital forensics is a valuable tool in homicide investigations since it can assist in the identification of suspects, the establishment of timelines, and the retrieval of lost or concealed material from digital devices. A significant benefit of digital forensics is its ability to frequently retrieve data that may have been erased or concealed. Specialized tools and techniques are employed by digital forensic specialists to retrieve deleted data, including the utilization of file carving techniques that can recover files even in cases where they have been overwritten or partially wiped. Additionally, it plays a crucial role in guaranteeing the acceptability of digital evidence in a court of law. In order for digital evidence to be accepted in court, it must meet specific legal criteria, including the authentication and dependability of the evidence, as well as the documentation of its custody from the moment it was gathered until it was presented in court.[10] Trained digital forensics professionals are responsible for ensuring that digital evidence adheres to legal requirements, which is crucial for securing a conviction in a criminal case.

Nevertheless, the application of digital forensics in criminal investigations also prompts significant inquiries over private rights and civil liberties. Electronic

[8] Baar van,R.van Beek, et. al, *Digital Forensics as a Service: A game changer. Digital Investigation* (May 11, 2014) *available at* - https://doi.org/10.1016/j.diin.2014.03.007. (last visited Sep. 17, 2024).
[9]A.Bendovschi, *Cyber-Attacks – Trends, Patterns and Security Countermeasures* (2020) *available at* - https://doi.org/10.1016/S2212-5671(15)01077-1. (last visited Sep 17, 2024).
[10]F.AMoussa, *Electronic evidence and its authenticity in forensic evidence* (2021) *available at* - https://ejfs.springeropen.com/articles/10.1186/s41935-021-00234-6. (last visited Sep. 17, 2024).

devices store a significant quantity of personal data, including contact information, messages, and photographs, and the utilization of digital forensic technologies can be extremely intrusive[11]. There is a potential for investigators to obtain data that is not directly relevant to the case, which could lead to breaches of privacy. Furthermore, the dependability and precision of digital evidence can be undermined by factors such as tampering, inaccuracies, or the intricacy of the analysis procedure.[12] This can lead to erroneous convictions or other instances of judicial error.

Hence, it is imperative to guarantee that the utilization of digital forensics in criminal inquiries is carried out in a manner that upholds privacy rights and civil liberties. This entails the implementation of policies and procedures to restrict the extent of digital forensics investigations, ensuring that investigators receive suitable training in digital forensics techniques, and establishing criteria for the acceptability of digital evidence in court.

Examples of Digital Forensics Tools and Techniques that may infringe on Privacy Rights:

While digital forensics is crucial for investigating and prosecuting cybercrimes, the utilization of specific tools and methods might encroach into the privacy rights of individuals. Here are a few instances of digital forensics technologies and approaches that could potentially violate privacy rights:

Data Carving:

Data carving is an essential technique in the field of digital forensics, predominantly employed to retrieve files that have been erased, damaged, or otherwise misplaced

[11] P. Reedy, *The risks for digital evidence. Strategic Leadership in Digital Evidence* (2021) *available at* - https://doi.org/10.1016/b978-0-12-819618-2.00012-7. (last visited Sep. 17, 2024).

[12] R. Stoykova,*Digital evidence: Unaddressed threats to fairness and the presumption of innocence* (Sep. 2021) *available at* - 105575. https://doi.org/10.1016/j.clsr.2021.105575. (last visited Sep. 18, 2024).

from digital storage devices such as hard disks, USB drives, and memory cards.[13] This approach relies on the identification and extraction of data by utilizing distinct file signatures, which are distinctive patterns of data associated with particular file formats (such as JPEG for photos, DOCX for Word documents, etc.).

The procedure entails scanning the storage medium for these distinctive patterns, and upon identification, the corresponding data is recovered, typically in fragments, from the storage device. Forensic professionals can utilize this capability to recreate files that are absent from the directory of the file system.[14] This is especially advantageous in cases when the file system is impaired or when files have been deliberately erased to hide evidence. Data carving is a highly valuable technique in investigations where digital evidence is crucial, as it can uncover many file kinds such as documents, photos, videos, and emails. It is frequently employed in court proceedings, corporate inquiries, and by law enforcement authorities to gather evidence.

Nevertheless, this approach has its limitations. Due to its indiscriminate nature, data carving has the potential to retrieve personal and sensitive information that is irrelevant to the investigation at hand. This unintentional retrieval gives rise to substantial privacy concerns, as it has the potential to expose confidential information of individuals who are unrelated to the case. Adhering to legal and ethical limitations, such as privacy laws and data protection requirements, is crucial while utilizing data carving in the field of digital forensics.

Furthermore, data carving does not consistently yield positive results. The fidelity and comprehensiveness of the retrieved files may fluctuate, particularly in cases where the storage device has sustained significant damage or if the data has been

[13] D. Povar, V.K. Bhadran, Forensic *Data Carving* (2011) *available at* - https://ui.adsabs.harvard.edu/abs/2011dfcc.conf..137P/abstract#:~:text=Identifying%20and%20recovering%20files%20based,the%20disk%20or%20digital%20media. (Last visited Sep. 18, 2024).

[14] Tariq, U., Ahmed, I., Bashir, A. K., et. al., *A Critical Cyber security Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review* (April 19, 2023) *available at* - https://doi.org/10.3390/s23084117. (last visited Sep. 18, 2024).

rewritten.[15] Notwithstanding these difficulties, data carving continues to be a potent instrument in the arsenal of digital forensics experts, serving a pivotal function in revealing digital evidence.

Keyword Searching:

Keyword searching is a method employed in digital forensics to locate particular keywords or phrases within digital media. This methodology can prove advantageous in discerning evidence pertaining to a certain crime or incident.[16] Nevertheless, keyword searching may inadvertently lead to the gathering of personal and sensitive data that is unrelated to the investigation. Collecting individuals' data in this manner can potentially infringe upon their privacy rights.

***Data Mining*:**

Data mining is a method employed in digital forensics to examine extensive datasets with the aim of detecting patterns or correlations.[17] Data mining has the potential to uncover significant evidence, but it can also lead to the gathering of personal and sensitive material that is irrelevant to the investigation. This can result in a breach of privacy for the individuals whose data is being gathered.

***Remote Access Tools**:*

Remote access tools are software applications that enable digital forensics investigators to remotely access and manipulate a device or system.[18] Although remote access technologies can be valuable for gathering evidence from a distant

[15]Alherbawi, N., Shukur, Z., & Sulaiman, R., *Systematic Literature Review on Data Carving in Digital Forensic. Procedia Technology* (2013) *available at* - https://doi.org/10.1016/j.protcy.2013.12.165. (last visited Sep. 17, 2024).
[16]Yinghua, G., Jill, S., et. al. *Validation and verification of computer forensic software tools—Searching Function* (2009) *available at* - https://doi.org/10.1016/j.diin.2009.06.015. (last visited Sep. 17, 2024).
[17] Thuraisingham, M. B., *Data Mining for Security Applications* (2017) *available at* - https://www.researchgate.net/publication/221452043_Data_Mining_for_Security_Applications. (last visited Sep. 19, 2024).
[18]Manson, J., *Remote Desktop Software as a forensic resource* (2022) *available at* - https://doi.org/10.1080/23742917.2022.2049560. (last visited Sep. 17, 2024).

site, their usage without legal authorization or for collecting unrelated personal or sensitive information might violate privacy rights.

Network Monitoring:

Network monitoring is a method employed in digital forensics to track network traffic with the purpose of detecting any dubious behaviour.[19] Although network monitoring can be valuable for detecting cybercrimes, it can also lead to the acquisition of personal and sensitive data that is unrelated to the inquiry. Collecting individuals' data in this manner can potentially infringe upon their privacy rights.

Hence, digital forensics plays a crucial role in the investigation and prosecution of cybercrimes. Nevertheless, the utilization of specific instruments and methodologies can violate the privacy rights of persons. Digital forensics investigators must employ these tools and procedures responsibly and ethically, ensuring that they refrain from gathering personal or sensitive data that is irrelevant to the inquiry.

Legislative Analysis of Digital Forensics on Privacy Rights and Civil Liberties

India

In India, digital forensics is governed by various legislations such as the *"*Information Technology Act, 2000, the Indian Evidence Act, and the Code of Criminal Procedure**.***"* These legislations provide guidelines for the "*collection, preservation, and analysis of digital evidence*," and aim to balance the need for digital forensics with the protection of privacy rights and civil liberties.

The Information Technology Act, 2000 (IT Act) is the primary statute in India that governs digital forensics. In the context of cybercrimes, the Act provides guidelines for the collection, preservation, and analysis of digital evidence. While the Act recognizes the need for digital forensics, it also seeks to balance this with the protection of privacy rights and civil liberties. One of the key provisions of the IT

[19]Sikos, L. F., *Packet analysis for network forensics: A comprehensive survey. Forensic Science International: Digital Investigation* (Mar. 2020) *avaialble at* - https://doi.org/10.1016/j.fsidi.2019.200892. (last visited Sep. 20, 2024).

Act is ***Section 43***[20]**,** which deals with unauthorized access to computer systems. This provision makes it an offense to access a computer system without authorization and provides for penalties for those who do so. This provision aims to safeguard the privacy rights of individuals by prohibiting unauthorised access to their computer systems**. Section 69**[21] of the IT Act, which addresses the interception and monitoring of digital communications, is another important provision, which authorises the government to intercept and monitor digital communications under certain conditions, such as in the interest of national security or to prevent the commission of a criminal offence. However, this monitoring and interception must be permitted by an appropriate authority and must be done in accordance with the procedure established by law. This clause aims to strike a balance between the need for digital forensics and the protection of privacy rights. ***Section 43A***[22] of the Information Technology Act, 2000, which provides for compensation when confidential personal data or information is not protected, clearly states that a body corporate has a legal responsibility to safeguard sensitive personal data or information when collecting, receiving, possessing, storing, handling, or dealing with it on a computer resource that it owns, controls, or operates Information sharing in violation of a valid contract is punishable under ***Section 72A***[23]of the Information Technology Act, 2000. According to this section, anyone who divulges personal information they have obtained while performing services under a valid contract without the person's consent will be subject to a fine of up to five lakh rupees, a term of imprisonment up to three years, or both.

However, there have been concerns raised about the potential infringement of privacy rights and civil liberties in the collection and analysis of digital evidence. For example, the use of data mining and keyword searching techniques could result in the collection of personal and sensitive information that is not relevant to the

[20] The Information Technology Act, 2000, S.43.
[21] The Information Technology Act, 2000, S. 69.
[22] The Information Technology Act, 2000, S. 43A.
[23] The Information Technology Act, 2000, S. 72A.

investigation.[24] Similarly, the use of remote access tools without proper authorization could result in the invasion of privacy of individuals. While the Information Technology Act, 2000 (IT Act) seeks to balance the need for digital forensics with the protection of privacy rights and civil liberties, there are several drawbacks to the Act that can result in a failure to maintain this balance. Some of these drawbacks include:

a. *Vague and ambiguous language*: The IT Act contains several provisions that use vague and ambiguous language, which can result in a lack of clarity in terms of what is allowed and what is not. This can lead to the misuse of digital forensics tools and techniques, resulting in the infringement of privacy rights and civil liberties.

b. *Lack of clear guidelines*: While the IT Act provides guidelines for the collection, preservation, and analysis of digital evidence, these guidelines are not always clear or comprehensive. This can result in confusion among digital forensics investigators, who may end up collecting or analyzing data in a manner that infringes on privacy rights and civil liberties.

c. *Lack of oversight***:** The IT Act does not provide for adequate oversight of digital forensics investigations. This can result in the misuse of digital forensics tools and techniques, without proper accountability or oversight.

d. *Limited scope of privacy protections*: The privacy protections provided by the IT Act are limited in scope and may not always be sufficient to protect the privacy rights and civil liberties of individuals. For example, the Act may not provide adequate protection against data mining or other advanced digital forensics techniques that can result in the collection of personal and sensitive information.

[24]Aldeen, Y. A. A. S., Salleh, M., et. al., *A comprehensive review on privacy preserving data mining* (Nov. 12, 2015) *available at* - https://doi.org/10.1186/s40064-015-1481-x. (last visited Sep. 17, 2024).

e. *Insufficient penalties*: The penalties for violating the privacy rights and civil liberties of individuals under the IT Act may not be sufficient to deter misconduct or provide adequate compensation for the harm caused.

Although the IT Act seeks to balance the need for digital forensics with the protection of privacy rights and civil liberties, there are several drawbacks to the Act that can result in a failure to maintain this balance. To address these drawbacks, it is important for the government to establish clear guidelines and oversight mechanisms for digital forensics investigations**,** and to provide adequate privacy protections and penalties for misconduct.

The Indian Evidence Act, 1872 (IEA) is one of the essential legislative enactments in India that governs the collection, maintenance and analysis of digital proof. The Indian Evidence Act (IEA) outlines the rules governing the admissibility of digital evidence in the judicial system. The Indian Evidence Act (IEA) acknowledges the utility of digital forensics in criminal investigations, yet it still strives to maintain a balance between this and the safeguarding of civil liberties and privacy rights. One of the key provisions of the IEA that is relevant to digital forensics is ***Section 65B***[25]**,** which deals with the admissibility of electronic records. This section provides that electronic records, including digital evidence, can be admitted as evidence in court if they are accompanied by a certificate in the prescribed format. The certificate must verify the authenticity of the electronic record and the manner in which it was collected and preserved. Another important provision of the IEA is ***Section 165***[26], which deals with the power of the court to order the production of documents. This section allows the court to order the production of documents, including digital evidence, in order to aid in the investigation or trial of a case. However, the court must balance the need for the evidence with the privacy rights and civil liberties of the individuals involved. The IEA also recognizes the importance of privacy rights

[25] The Indian Evidence Act, 1872, S.65B.
[26] The Indian Evidence Act, 1872, S. 165.

and civil liberties in the context of digital forensics. ***Section 24***[27]of the Act provides that no confession made by any person to a police officer shall be admissible as evidence against that person. This provision ensures that individuals are not compelled to provide self-incriminating evidence and that their privacy rights are protected. However, there are several challenges to maintaining a balance between digital forensics and privacy rights and civil liberties under the IEA. For example, the use of advanced digital forensics techniques, such as data mining and keyword searching, can result in the collection of personal and sensitive information that is not relevant to the investigation. Similarly, the use of remote access tools without proper authorization can result in the invasion of privacy of individuals. To address these challenges, it is important for digital forensics investigators to be trained in the proper use of digital forensics tools and techniques, and to ensure that they are not collecting personal or sensitive information that is not relevant to the investigation. Additionally, it is important for the courts to balance the need for digital evidence with the privacy rights and civil liberties of individuals, and to ensure that the admissibility of digital evidence is based on proper certification and authentication.

The Code of Criminal Procedure (CrPC) provides the procedural framework for conducting criminal investigations and trials in India. It is relevant to digital forensics, privacy rights, and civil liberties in several ways.

Firstly, ***Section 91*** *of the Code of Criminal Procedure (CrPC)*[28] grants the authority to assign summons or create written orders for the production of documents, which may include electronic records that are essential for the investigation or trial. This provision allows law enforcement agencies to obtain digital evidence for investigation purposes, but it also imposes restrictions on the use of such evidence to protect privacy rights and civil liberties. The provision requires that the summons or written order must be for a specific purpose, and the production of the evidence

[27] The Indian Evidence Act, 1872, S. 24.
[28] The Code of Criminal Procedure, 1973, S.91.

must not be unreasonable or oppressive. Secondly, ***Section 165***[29] of the CrPC empowers police officers to conduct searches of electronic devices during an investigation, subject to certain conditions. This provision requires that the officer conducting the search must have reason to believe that the device contains evidence related to the offence being investigated, and that the search must be conducted in the presence of two or more independent witnesses. This provision protects the privacy rights of individuals by imposing limitations on the scope of the search and by requiring the presence of independent witnesses during the search. Thirdly, *Section 207*[30] of the CrPC provides for the provision of electronic copies of documents and records to accused persons during the trial. This provision ensures that accused persons have access to digital evidence that is being relied upon by the prosecution in the trial, thereby protecting their rights to a fair trial and due process. Finally, *The Code of Criminal Procedure (CrPC) stipulates in Section 41D*[31] that police officers must notify the individual in question of the rationale behind the arrest, along with the right to legal counsel and the right to obtain a lawyer at the time of their interrogation. The Code of Criminal Procedure Chapter V provides safeguards for individuals' civil liberties by ensuring that they are apprised of their legal rights during the inquiry and trial process.

While the Code of Criminal Procedure (CrPC) provides a framework for the use of digital forensics in criminal investigations and trials, there are also some drawbacks that may impact privacy rights and civil liberties. One of the main drawbacks is the *lack of clear guidelines* for the admissibility of digital evidence. While the CrPC provides for the production of electronic records and the use of digital evidence in investigations and trials, there are no clear guidelines for the admissibility of such evidence.[32] This can result in inconsistencies in the treatment of digital evidence and

[29] The Code of Criminal Procedure, 1973, S. 165.
[30] The Code of Criminal Procedure, 1973, S. 207.
[31] The Code of Criminal Procedure, 1973, S. 41D.
[32]Moussa, A. F., *Electronic evidence and its authenticity in forensic evidence* (Aug. 27, 2021) *available at* - https://doi.org/10.1186/s41935-021-00234-6. (last visited Sep. 17, 2024).

may lead to the violation of privacy rights and civil liberties. Another drawback is the *potential for misuse of digital evidence by law enforcement agencies*. Digital evidence can be easily tampered with or fabricated, and there have been cases where law enforcement agencies have planted digital evidence to secure convictions[33]. This can lead to the violation of privacy rights and civil liberties of individuals who are wrongly accused or convicted based on false digital evidence.

Additionally, there are *concerns about the collection and retention of digital data by law enforcement agencies.* Digital data can be sensitive and may contain personal information, and there is a risk that such data can be misused or abused by law enforcement agencies.[34] There is a need for clear guidelines on the collection, retention, and use of digital data to ensure that privacy rights and civil liberties are protected.

Finally, *the lack of expertise in digital forensics* among law enforcement agencies can also be a drawback. Digital forensics is an intricate discipline necessitating particular knowledge and aptitudes, and in some cases law enforcement agencies may not be adequately equipped to manage digital evidence suitably. The possible mishandling of digital evidence can lead to inaccuracies, which can have ramifications on the safeguarding of individual privacy rights and civil liberties[35].

Consequently, although the Criminal Procedure Code offers a model for the use of digital forensics in criminal investigations and proceedings, there are also shortcomings that must be confronted to guarantee that personal privacy rights and civil liberties are safeguarded. It is necessary to establish explicit guidelines

[33]Gonzales, D., Grier, J., et. al., *New Approaches to Digital Evidence Acquisition and Analysis* (2018) *available at* - https://nij.ojp.gov/topics/articles/new-approaches-digital-evidence-acquisition-and-analysis. (last visited Sep. 18, 2024).
[34]Kröger, J. L., Miceli, M., et. al., *How Data Can Be Used Against People: A Classification of Personal Data Misuses*(2021) *available at* - https://doi.org/10.2139/ssrn.3887097. (last visited Sep. 22, 2024).
[35]Ningsih, S., *Digital Forensics Workflow as A Mapping Model for People, Evidence, and Process in Digital Investigation*(2018) *available at* - https://doi.org/10.17781/p002463. (last visited Sep. 22, 2024).

pertaining to the admissibility of digital evidence, ensure the protection against potential abuse of digital evidence, formulate regulations for the compilation and keeping of digital data, and supply law enforcement agencies with advanced digital forensics expertise.

United States

The use of digital forensics in the United States for investigations and prosecutions of criminal activity has raised significant privacy rights and civil liberties concerns. As a result, there have been several legislative initiatives to address these concerns.

One such initiative is "*the Electronic Communications Privacy Act (ECPA)*," which was enacted in 1986. The ECPA updated federal wiretap laws to address new technologies, such as email, and introduced provisions for obtaining digital evidence through the use of search warrants. However, the ECPA has been criticized for being outdated and inadequate in protecting privacy rights and civil liberties in the digital age[36]. To address these concerns, the U.S. Congress has introduced several bills to update the ECPA, such as "the *Email Privacy Act and the Online Communications and Geolocation Protection Act."* These bills seek to update the ECPA by requiring law enforcement agencies to obtain a warrant before accessing digital content and communications, and by providing additional protections for location data.[37]

Additionally, the *USA PATRIOT Act*, enacted in 2001, allows law enforcement agencies to conduct surveillance and obtain digital evidence without a warrant in certain circumstances. In addition to this, concerns about possible invasions of civil liberties and privacy have been made by this. To address these concerns, "*the USA FREEDOM Act"* was enacted in 2015, which imposed new restrictions on the

[36]Ohm, P. , *Electronic Surveillance Law and the Intra-Agency Separation of Powers* (2012) *available at* - https://core.ac.uk/download/pdf/216988611.pdf. (last visited Sep. 22, 2024).
[37]Scolnik, A., P*rotections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*(2009) *available at* - https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4471&context=flr. (last visited Sep. 22, 2024).

collection of digital data and increased transparency requirements for government surveillance programs.[38]

Another important legislative initiative is the *Cyber security Information Sharing Act (CISA)***,** enacted in 2015, which provides a framework for private entities to share digital data with the government for cyber security purposes. However, CISA has been criticized for its potential impact on privacy rights and civil liberties, particularly with regard to the sharing of personal data.[39]

The Fourth Amendment of the U.S. Constitution acts to safeguard citizens from unwarranted searches and seizures, including those that involve digital information. The implications and implementation of the Fourth Amendment in the digital age have been extensively explored both in terms of discourse and legal action.

In the United States, the legislative initiatives related to digital forensics, privacy rights, and civil liberties reflect the necessity of striking a delicate balance between law enforcement requirements and individual liberties. Despite considerable attempts to adjust laws and regulations to address these issues, there is still a requirement for persistent monitoring and assessment to guarantee that privacy rights and civil liberties are upheld in the digital world.

- ***Comparative Analysis: India and USA***

Legislative Analysis	**India**	**USA**
Clear guidelines for digital evidence	Guidelines exist, but they are not comprehensive.	The Electronic Communications Privacy Act (ECPA) provides clear guidelines for

[38] Pope, P.& Fisher, D., *Surveillance and Wiretapping* (2017) *available at* - https://www.mtsu.edu/first-amendment/article/1153/surveillance-and-wiretapping. (last visited Sep. 23, 2024).

[39]Pala, A., Zhuang, J, *Information Sharing in Cyber security: A Review* (2021) *available at* - https://www.researchgate.net/publication/335009845_Information_Sharing_in_Cybersecurity_A_Review. (last visited Sep . 22, 2024).

		obtaining digital evidence through search warrants.
Protections for privacy rights	Recent Digital Personal Data Protection Act 2023 is an exclusive right for the purpose of Privacy Rights protect but still there exist loopholes via which privacy rights can be infringed.	The Privacy Act, which regulates the acquisition and use of personal information, provides enhanced protections.
Transparency and accountability	Limited transparency and accountability in government surveillance programs.	Legislation such as the Foreign Intelligence Surveillance Act that make provisions for accountability and transparency in government surveillance programmes.
Balancing law enforcement needs with individual rights	Unbalanced relationship between law enforcement requirements and individual liberties.	Strives to balance law enforcement needs with individual rights, particularly with regard to the search and seizure of digital data.
Admissibility of digital evidence	Digital evidence admissibility is subject to legal procedures and regulations.	The admissibility of digital evidence is regulated by legal processes and regulations, with explicit directives

		given by the Federal Rules of Evidence.
Chain of custody	Chain of custody is important, but procedures can be improved.	The meticulous maintenance of the chain of custody ensures the authenticity and admissibility of digital evidence.
Bias and accuracy	Digital forensics can be subject to bias and accuracy issues.	Strives to conduct investigations in an objective and unbiased manner, with emphasis on accurate analysis and interpretation of digital evidence.
Ethical considerations	Ethical considerations are taken into account, but they are not comprehensive.	Ethical considerations are taken into account, particularly with regard to privacy rights and civil liberties.

Case Studies:

There are various case studies illustrating the complex and nuanced relationship between digital forensics, privacy rights, and civil liberties. These case-studies are very important for the purpose of understanding the impact of digital forensics on privacy rights and civil liberties.

***The Pegasus Spyware Case*:** In 2021, a consortium of international journalists reported that the Pegasus spyware, developed by Israeli firm NSO Group, had been

used to target hundreds of individuals in India, including journalists, human rights activists, politicians, and business executives. The spyware is capable of infiltrating smart phones and collecting a wide range of data, including text messages, emails, and call records[40]. The use of the spyware raised concerns about the violation of privacy rights and civil liberties, as well as the potential abuse of the technology for political purposes.

The Delhi Riots Case: In 2020, the Delhi Police used digital forensics to investigate the riots that broke out in the city. The police used CCTV footage, social media posts, and call records to identify and arrest[41]. However, the use of digital forensics also raised concerns about privacy rights and civil liberties, as the police reportedly accessed the social media accounts of individuals without a warrant and used facial recognition technology to identify suspects.

***The Bhima Koregaon Case*:** Several human rights activists were arrested in Maharashtra in 2018 in association with the Bhima Koregaon violence. The police claimed to have found incriminating evidence on the activists' electronic devices, including emails and WhatsApp conversations[42]. However, the use of digital forensics in the case raised concerns about privacy rights and civil liberties, as the activists claimed that their devices had been planted with the evidence and that the police had violated their right to privacy.

[40]Priest, D., Timberg, C., et. al., *Private Israeli spyware used to hack cellphones of journalists, activists worldwide* (2021) *available at* - https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/. (last visited Sep. 22, 2024).

[41]Mani, G., *Technology used extensively to investigate northeast Delhi riots cases: Police chief SN Shrivastava*(2021) *available at* - https://www.newindianexpress.com/cities/delhi/2021/feb/19/technology-used-extensively-to-investigate-northeast-delhi-riots-cases-police-chiefsn-shrivastava-2266184.html. (last visited Sep. 22, 2024).

[42]Deb, S., T*he unravelling of a conspiracy: were the 16 charged with plotting to kill India's prime minister framed?*(2021) *available a*t - https://www.theguardian.com/world/2021/aug/12/bhima-koregaon-case-india-conspiracy-modi. (last visited Sep. 18, 2024).

Cybercrime Investigations: In 2016, the Federal Bureau of Investigation (FBI) requested Apple to develop a means for bypassing the encryption of an iPhone linked to one of the San Bernardino attackers. Apple refused to comply, due to considerations for user privacy and security. The ultimate outcome of the dispute over the FBI's endeavour to access the iPhone through an independent provider posed queries pertaining to the precarious balance between fulfilling law enforcement duties and safeguarding private rights and freedoms[43].

***Terrorism investigations*:** Following the 9/11 attacks, the USA PATRIOT Act facilitated the expansion of surveillance capacity for law enforcement agencies, authorising them to conduct surveillance on persons suspected to be involved in terrorist activity without obtaining a warrant[44]. These powers have been used to collect digital evidence, such as emails and social media activity, in terrorism investigations. However, these powers have also been criticized for infringing on privacy rights and civil liberties.

Police investigations: In 2013, the New York City Police Department (NYPD) was sued for its use of the controversial "stop and frisk" policy, which involved stopping and searching individuals without probable cause. The NYPD used data mining and predictive analytics tools to identify individuals who were likely to commit crimes based on factors such as age, race, and location[45]. The use of these tools raised concerns about bias and infringement on privacy rights.

[43]Nakashima, E.& Albergotti, R., *The FBI wanted to unlock the San Bernardino shooter's iPhone. It turned to a little-known Australian firm* (2021) *available at* - https://www.washingtonpost.com/technology/2021/04/14/azimuth-san-bernardino-apple-iphone-fbi/. (last visited Sep. 22, 2024).

[44]Pope, P.& Fisher, D., *Surveillance and Wiretapping* (2017) *available at* - https://www.mtsu.edu/first-amendment/article/1153/surveillance-and-wiretapping. (last visited Sep. 22, 2024).

[45]Ferrandino, A.J., *The effectiveness and equity of NYPD stop and frisk policy* (2014) *available at* - https://www.researchgate.net/publication/309517292_The_effectiveness_and_equity_of_NYPD_stop_and_frisk_policy_2003-2014. (last visited Sep. 23, 2024).

Employee monitoring: Employers often use digital forensics tools to monitor employee activity on company devices and networks. While employers have a legitimate interest in monitoring employee activity to ensure productivity and prevent misconduct, these practices can also infringe on employee privacy rights. For example, in 2016, a court ruled that a company violated an employee's privacy rights by using a key logger to monitor his computer activity without his knowledge.[46]

The case examples presented above illustrate the intricate and nuanced link between digital forensics, privacy rights, and civil liberties. Digital forensics provides law enforcement authorities with a practical method to analyze, investigate, and legally pursue criminal actions, such as terrorism and cybercrime.[47] On the other hand, the introduction of digital forensics might give rise to apprehensions regarding civil liberties and personal privacy, particularly when there are no adequate safeguards and oversight in place. Striking a careful balance between the need for digital evidence and the protection of personal liberties is a substantial endeavour that requires the establishment of appropriate measures, monitoring, and responsibility.

Conclusion and Suggestions

The impact of digital forensics on the protection of private rights and civil liberties is a multifaceted issue that requires meticulously planned action. The application of digital forensics can be an invaluable asset for law enforcement agencies; but it can also result in the violation of private data and communication, so impacting personal privacy and civil liberties[48]. In order to address these concerns, it is crucial to

[46]Wen, H. J., Schwieger, D., & Gershuny, P., *Internet Usage Monitoring in the Workplace: Its Legal Challenges and Implementation Strategies* (Mar. 30, 2007) *available at* - https://doi.org/10.1080/10580530701221072. (last visited Sep. 24, 2024).

[47] Hinduja, S., *Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future* (2007) *available at* - https://www.cybercrimejournal.com/pdf/sameer.pdf. (last visited Sep. 24, 2024).

[48]Sotiroski, L., *Cyber Security Protection and Implementing of Legal Framework* (2018) *available at* -

establish clear legal frameworks and monitoring procedures. These processes should guarantee that digital evidence is acquired using legitimate methods, with proper authority and supervision. Furthermore, with the continuous advancement of technology, the influence of digital forensics on privacy and civil rights is expected to grow increasingly intricate and difficult to tackle, necessitating continuing discussions and cooperation among all parties involved.[49] Striking a balance between carrying out efficient criminal investigations and safeguarding privacy and civil liberties is a challenging endeavour that necessitates an advanced understanding of the advantages and disadvantages of digital forensics. It also demands a dedication to discovering resolutions that uphold both privacy and security. [50]

Balancing privacy rights and criminal investigations is a complex issue that requires careful consideration of both individual rights and the needs of law enforcement agencies. Few of the suggestions and recommendations that might prove helpful in dealing with the complexity:

Strengthen legislative frameworks: There is a need to strengthen the legislative framework to ensure that the rights of citizens are protected while still allowing law enforcement agencies to carry out their duties. This can be done by setting clear guidelines on the use of digital forensics, outlining the rights of citizens, and establishing a regulatory framework to oversee the use of such technology.

Establish independent oversight bodies: Independent oversight bodies that can monitor the use of digital forensics by law enforcement agencies needs to be

https://www.academia.edu/41982650/cyber_security_protection_and_implementing_of_legal_framework. (last visited Sep. 24, 2024).

[49]Rodrigues, R., *Legal and human rights issues of AI: Gaps, challenges and vulnerabilities* (Dec.4, 2020) *available at* - 100005. https://doi.org/10.1016/j.jrt.2020.100005. (last visited Sep. 24, 2024).

[50]Bird, E., Fox, J., et. al., *The ethics of artificial intelligence: Issues and initiatives*(2020) *available at* - https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf. (last visited Sep. 25, 2024).

established. These bodies should be empowered to investigate any misuse of technology and take appropriate action to ensure that privacy rights are protected.

Provide training and education: Law enforcement agencies should be provided with comprehensive training and education on the use of digital forensics. This will aid in guaranteeing that inquiries are conducted in a way that accords proper deference to individuals' rights and privacy.

Encourage public participation: The public should be encouraged to participate in the development of legislative frameworks and policies related to digital forensics. This will help to ensure that the needs of citizens are taken into account and that privacy rights are protected.

Foster international cooperation: India and the USA should collaborate in order to establish shared protocols and norms pertaining to the utilisation of digital forensics within criminal inquiries. This will help to prevent discrepancies in the application of technology and ensure that privacy rights are protected on a global scale.

Foster technological innovation: Both countries should continue to foster technological innovation in the field of digital forensics. This can help to create new tools and techniques that are more effective and less invasive, thus reducing the impact on individual privacy rights.

India and the USA can attain a balance between protecting the right of privacy of individuals and fulfilling the demands of law enforcement agencies by taking the appropriate steps. This will contribute to the awareness of upholding justice and safeguarding the primary rights of citizens.