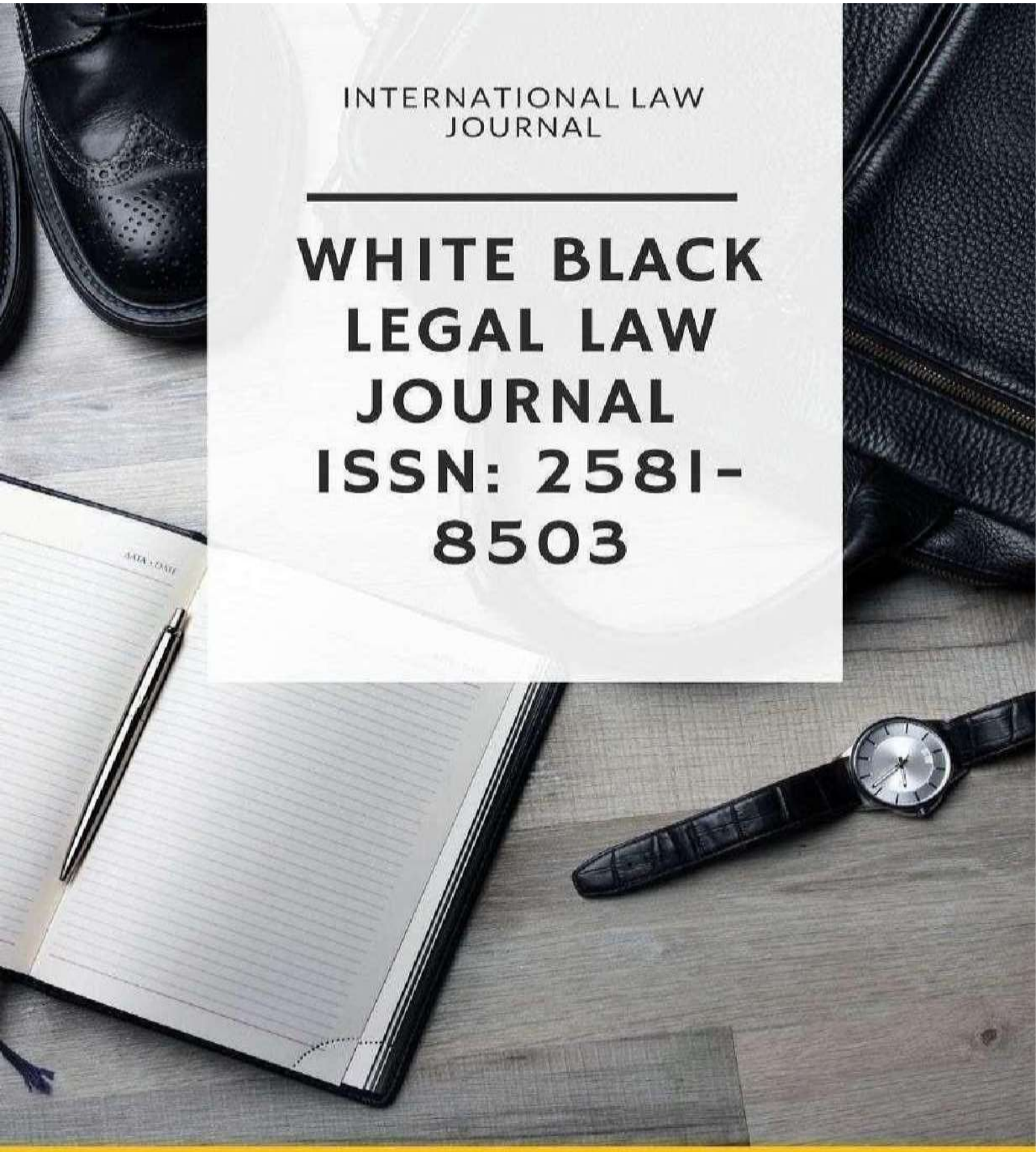

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi, Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur,
M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

"THREATENING CALL AND ITS FORENSIC ANALYSIS"[1]

AUTHORED BY: KUMAR KARAN
Affiliation: Chanakya National Law University, Patna
Designation: Masters of Law (2023-24)

ABSTRACT

This abstract outlines the forensic analysis of a threatening phone call, elucidating the methodology employed to dissect the call's origin and authenticity. Leveraging advanced forensic techniques, the investigation delves into voice recognition, signal triangulation, and metadata scrutiny to ascertain the caller's identity and intent. The study aims to contribute to the evolving field of digital forensics, offering insights into the challenges posed by threatening communications and providing a framework for law enforcement to address such incidents effectively.

Keywords: triangulation, metadata

INTRODUCTION

In the modern digital age, communication has evolved significantly, encompassing various mediums that include not only traditional voice calls but also electronic means. However, along with the positive advancements, there has been an increase in instances of threatening calls, a form of communication that can lead to distress, fear, and potential harm. A threatening call involves the use of communication technology to intimidate, harass, or instill fear in the recipient through verbal threats, derogatory language, or explicit content. Such calls have serious psychological and sometimes physical consequences for the victim.

Forensic analysis plays a crucial role in addressing this issue, employing a scientific approach to unravel the intricacies of threatening calls. By employing advanced techniques, experts can analyze various facets of the communication, such as the caller's identity, location, and intent. This process

[1]Kumar karan, LLM Student, Chanakya National Law University.

involves a comprehensive examination of call metadata, voice characteristics, language patterns, and contextual information to establish a solid foundation for legal actions.

This study delves into the realm of threatening calls and their forensic analysis. It aims to explore the methodologies and technologies employed to uncover vital information hidden within these communications, shedding light on the identity of the perpetrator and their motivations. Furthermore, the study will discuss the legal implications, ethical considerations, and the evolving landscape of forensic analysis in a digital age.

Through a multidisciplinary approach, combining elements of psychology, technology, and law, this study seeks to provide a comprehensive understanding of threatening calls, their impact, and the vital role forensic analysis plays in bringing perpetrators to justice and providing victims with the reassurance they deserve in an increasingly interconnected world.

Background and Context of Threatening Calls

Types of Threatening Calls:

Personal Threats: These involve threats directed at an individual, often for personal reasons such as revenge, anger, or harassment.

Bomb Threats: Calls claiming that a bomb or explosive device is present, typically intended to create fear, panic, or disruption.

Extortion Calls: Calls demanding money or valuables in exchange for not carrying out harm, often directed at businesses or individuals.

Cyber Threats: Threats made online or over the phone, which may include hacking, doxxing (revealing personal information), or spreading false information.

Hate Speech and Harassment: Calls that contain hate speech or harassment based on a person's race, religion, gender, or other characteristics.

FORENSIC ANALYSIS OF THREATENING CALLS[2]

ROLE OF FORENSICS IN CRIMINAL INVESTIGATIONS

Forensic analysis plays a crucial role in criminal investigations, including those involving threatening calls. Forensic experts use various techniques and methods to examine evidence related to these calls,

[2] **Forensic Communication: Application of Communication Research to Courtroom Litigation" by Peter T. Forni:** This book discusses various aspects of forensic communication, including the analysis of threatening calls and their use in legal proceedings.

with the aim of identifying the perpetrator, collecting evidence for legal proceedings, and ensuring a fair and just resolution to the case. Here's an overview of the role of forensics in the analysis of threatening calls:

1. Call Trace and Location Analysis: Forensic experts can trace the origin of threatening calls by analyzing call records and metadata. This includes identifying the caller's phone number, location, and the network used for the call. Location analysis may involve cell tower triangulation or GPS data to pinpoint the caller's whereabouts.
2. Voice Analysis: Voice analysis is a critical component of forensic investigation for threatening calls. Experts can analyze the audio recordings of calls to:Determine the speaker's gender, age, and emotional state.Compare the caller's voice to known samples, such as voice recordings of suspects or individuals of interest.Identify distinctive speech patterns, accents, or speech impediments that may provide clues to the caller's identity.
3. Linguistic and Content Analysis: Linguistic experts can analyze the language, content, and writing style used in threatening calls. This analysis may include identifying specific words or phrases, profanity, threats, or references that could reveal information about the caller's background, motives, or potential connections to the victim.
4. Digital Forensics: In cases involving digital threats, such as emails or text messages, forensic experts can analyze digital evidence, including.IP addresses and email headers to trace the source of electronic communication.Metadata from digital files (e.g., image or video files) that may contain information about the device or location where the file was created.Deleted or hidden data that may be relevant to the investigation.
5. Cyber Forensics: In cases of cyber threats and online harassment, cyber forensics experts examine digital evidence related to the threats, such as:Email headers and server logs,Social media messages, posts, and profiles,Digital footprints, including the use of anonymous proxies or VPNs,Malware or hacking tools used in the threats.
6. Data Recovery: Forensic experts may employ data recovery techniques to retrieve deleted or damaged digital evidence, such as text messages, call logs, or images.

METADATA EXAMINATION: TRACKING CALL ORIGIN AND TIMESTAMPS[3]

Metadata examination, particularly in the context of threatening calls, involves the analysis of information associated with the call, such as call origin and timestamps. This metadata can be valuable for tracking the source of the call, establishing timelines, and providing evidence in investigations. Here's how metadata examination can help in tracking threatening calls:

Call Origin Analysis:

Metadata often includes data about the call's origin, such as the caller's phone number, network identifier, and geographic location.Analyzing call origin data can help identify the location from which the call was made, which can be crucial for narrowing down potential suspects or witnesses.

Timestamp Analysis:

Metadata includes timestamps that record the date and time when the call was made.

Examining timestamps can establish a timeline of communication events, helping investigators understand the sequence of threatening calls and their relationship to other relevant events or incidents.

Duration of Calls:

Longer calls may suggest more in-depth discussions or threats, while shorter calls may indicate brief and direct communication.

Frequency and Patterns: Analyzing the timestamps and call duration can reveal patterns of communication, such as the frequency of threatening calls.

Tracking Spoofed Numbers: In cases where the caller's number is spoofed or hidden, metadata examination may involve tracking the source of the spoofing or efforts to obscure the caller's identity.

Corroboration with Other Evidence:Metadata is often used in conjunction with other forms of evidence, such as voice recordings, digital evidence, and witness statements, to build a comprehensive case against the threat-maker.

[3] [3] **Forensic Analysis of Voice Stress Analyzer Admissibility in US Courts: A Case Study" by Michael G. Caligiuri, J. Steven Wormith, and Craig Bennell**

TOOLS AND TECHNOLOGIES FOR THREATENING CALL ANALYSIS

Call Detail Record (CDR) Analysis:

1. Investigators use CDR analysis tools and software to examine call metadata, trace call paths, and determine the source of threatening calls. It helps establish communication patterns and timelines.
2. Voice Biometrics Software:
3. In threatening call analysis, voice biometrics tools can be used to compare the caller's voice to known voice samples, potentially identifying the caller even when using different phone numbers or disguising their voice.
4. Advanced Audio Enhancement Techniques:
5. Enhancing audio quality is essential for accurately transcribing and analyzing threatening calls. Techniques include noise reduction, echo cancellation, and clarity enhancement to make voices more intelligible.
6. 4. Forensic Linguistics Software:
7. These tools help identify linguistic patterns, analyze content, and compare written threats to known samples or profiles, aiding in the identification of the threat-maker.
8. 5. Metadata Analysis Tools:
9. These tools help trace call paths, establish timelines, and determine if the caller's phone number has been spoofed or altered to hide their identity.
7. Audio Authentication Software:
10. In threatening call analysis, this type of software can confirm that audio recordings have not been tampered with or altered, ensuring the integrity of evidence.
8. Cell Tower and GPS Tracking Tools:
11. These tools help determine the geographic location of the caller, especially when calls are made from mobile devices. They can be instrumental in pinpointing the caller's whereabouts.
9. Digital Forensic Software:
12. Investigators use these tools to extract, examine, and analyze digital evidence for threats and harassment, including IP addresses, message content, and timestamps.
10. Automated Voice Analysis Software:
13. While not as comprehensive as voice biometrics, these tools can help identify potential

matches in voice recordings based on acoustic features.

CHALLENGES AND LIMITATIONS IN THREATENING CALL ANALYSIS

1. Anonymous Callers and Spoofing Techniques:

Challenge: Anonymous callers who deliberately hide their identities pose a significant challenge. They may use techniques such as caller ID spoofing, voice distortion, or disposable phones to conceal their true identities.

Limitation: Tracing and identifying anonymous callers can be extremely difficult, as they take measures to evade detection. Law enforcement may need cooperation from telecom companies and the use of advanced tracing techniques.

2. Technical Limitations in Audio Enhancement and Speaker Identification:

Challenge: Audio recordings of threatening calls may have poor quality, background noise, or interference, making it challenging to enhance audio for clear analysis.

Limitation: Despite advanced audio enhancement techniques, some recordings may remain unintelligible, making it difficult to analyze the content or identify the caller. Additionally, voice recognition and speaker identification accuracy may vary depending on the quality of the recording.

3. Jurisdictional and Cross-Border Challenges in Digital Forensics:

Challenge: Threatening calls often transcend geographical boundaries, and digital evidence may be stored or routed through servers in different jurisdictions.

Limitation: Jurisdictional differences in laws and regulations can hinder the collection and sharing of evidence. International cases may require cooperation between law enforcement agencies in different countries, which can be complex and time-consuming.

4. Data Privacy Concerns:

Challenge: Collecting and analyzing digital evidence, including call records and digital communications, must comply with data privacy regulations.

Limitation: Privacy concerns can limit the extent to which investigators can access and use certain types of evidence, especially when dealing with personal data or communications.

5. Legal Admissibility of Evidence:

Challenge: Ensuring that evidence obtained through digital forensics and call analysis is admissible in court can be challenging.

Limitation: Evidence may be deemed inadmissible if proper chain of custody, forensic protocols, or legal procedures are not followed. This can weaken the case against the perpetrator.

6. Rapidly Evolving Technology:

Challenge: Technology used by anonymous callers and cybercriminals is constantly evolving.

Limitation: Law enforcement and forensic experts must continually adapt their techniques and tools to keep pace with emerging technologies and tactics used by threatening call perpetrators.

7. Resource Constraints:

Challenge: Law enforcement agencies may have limited resources, including personnel, expertise, and funding, dedicated to threatening call investigations.

Limitation: Limited resources can affect the speed and effectiveness of investigations, particularly in cases with a high volume of threats or complex digital evidence.

CONCLUSION: FUTURE TRENDS AND TECHNOLOGICAL ADVANCES

1. Advancements in Voice and Speech Recognition Technology:

Future Trend: Voice and speech recognition technology is expected to become more accurate and versatile.

Impact: Improved voice recognition algorithms will enhance the ability to identify and authenticate callers. This technology will be particularly valuable for identifying threatening call perpetrators even if they attempt to disguise their voices. Additionally, it may help in real-time monitoring of voice communications for potential threats.

2. Integration of AI and Machine Learning in Threat Analysis:

Future Trend: AI and machine learning will play a growing role in threat analysis and risk assessment.

Impact: These technologies will enable more efficient and automated analysis of threatening calls and messages. Machine learning algorithms can help identify patterns, anomalies, and linguistic characteristics associated with threats, streamlining the investigative process and enhancing accuracy. AI-driven chatbots and virtual assistants may also be used to assist victims and gather preliminary information.

3. Potential Impact of 5G Technology on Digital Forensic Procedures:

Future Trend: The rollout of 5G technology will bring faster, more reliable, and widespread connectivity.

Impact: 5G networks will enable quicker data transfer, which can expedite the collection and transmission of digital evidence. Additionally, the proliferation of IoT (Internet of Things) devices

connected to 5G networks may increase the volume of potential digital evidence sources, requiring forensic experts to adapt their techniques and tools.

4. Use of Blockchain for Evidence Integrity:

Future Trend: Blockchain technology, known for its data immutability and security features, may find applications in preserving the integrity of digital evidence.

Impact: Blockchain can help maintain a transparent and unchangeable record of evidence custody and handling, ensuring the tamper-proof status of digital evidence.

5. Improved Data Visualization and Presentation:

Future Trend: Data visualization tools will continue to advance, making it easier to present complex digital forensic findings in a comprehensible manner.

Impact: Clear and effective data visualization can aid investigators, legal professionals, and jurors in understanding the significance of digital evidence, potentially leading to more successful prosecutions.

6. Increased Emphasis on Cybersecurity in Threat Analysis:

Future Trend: As threats increasingly originate from digital sources, the integration of cybersecurity practices into threat analysis will grow.

Impact: Enhanced cybersecurity measures will help protect digital evidence from tampering and secure communication channels used in investigations. Ensuring the security of digital evidence will be a critical aspect of maintaining its integrity.

7. Big Data Analytics in Threat Assessment:

Future Trend: The use of big data analytics will expand to include threat assessment and risk management.

Impact: By processing vast amounts of data from various sources, including social media and communication records, big data analytics can help identify potential threats more proactively. It can also assist in identifying trends and patterns related to threatening behaviors.

These future trends and technological advancements will continue to shape the landscape of threatening call analysis and digital forensics. As technology evolves, professionals in these fields will need to stay updated with the latest tools and methodologies to effectively combat threats and ensure the integrity of digital evidence.