Legal Implications and Challenges of Forensic Analysis and Digital Data under New Criminal Laws

VAIBHAV PANDEY[1], JYOTI YADAV[2]
[1, 2]*Deen Dayal Upadhyaya Gorakhpur University Gorakhpur*

Abstract*— The recent passage of the Bharatiya Nyaya Sanhita 2023, the Bharatiya Nagarik Suraksha Sanhita 2023, and the Bharatiya Sakshya Adhiniyam 2023 marks an important transformation of the criminal justice system in India. These laws are designed to modernize the criminal code, enhance public safety, and improve the rules of evidence. The new legislation focuses on a revision of statutory definitions of crime, a quicker process for adjudication, improvements in technologies related to policing, and better protections for victims of crime. To that end, the reforms to the field have been opposed by concerns regarding implementation, reflecting on the nationwide lack of resources and training to efficiently oversee police practices and structure criminal proceedings. Defined police powers and authorities imposed by the legislative reform also raise concerns regarding the possibility of misuse, infringement on privacy, and encroachment on civil liberties. With some emphasis on efficiency in forwarding criminal processes, critics note that it confounds an already strained judicial process and seek to assuage fears surrounding a judicial backlog. Concerns around engagement with marginalized communities vis-à-vis legitimacy of sentencing, present systemic discretion in policing towards particular communities and minorities, resulting in negative engagement with the implicit bias that the legislation intends to address. Further, the lack of clarity around criminal criminalization, or rapidly changing the law without engagement through notice and understanding, raises issues surrounding lagging criminal sanctions and constitutional reappearances. Addressing these issues will be crucial to establishing the reforms as successful in achieving their objectives, without these individuals encountering their limitations - or other unintended consequences.

Index Terms- Accountability, Advanced Technology, Civil Liberties, Constitutional Issues, Data Collection, Expedited Trials, Implementation Challenges, Judicial Backlog, Legal Ambiguities, Legal Challenges, Privacy Concerns, Transparency, Victim Protection

I. INTRODUCTION

India is ushering in a new phase of legal reform through the enactment of three new laws: the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, and the Bharatiya Sakshya Adhiniyam, 2023. These laws, which came into force on July 1, 2024, represent a complete overhaul of India's criminal justice system to cater to contemporary issues and shift from age-old legal processes toward our current state of affairs. The latest criminal law reforms in India represent an important step towards meeting these demands. The new reform process aims to modernize the legal structure in several important ways. First, the reforms address the responsiveness of the integrity of the justice system. In order to operate in a contemporary era, law can and must be adaptable to today's reality; this includes the nature of contemporary issues relating to crime and social change. For instance, today's rise in digital crime and the continued re-shaping of social norms; the reforms are intended to assure that the legal structure is able to manage new types of criminal activity, and societal social justice to meet changing expectations at the same time. Second, the reforms are aimed at equity within the justice process. There have historically been aspects of laws that are unbalanced, that often privilege certain groups of people over others, while failing to protect the rights and privileges of marginalized certain groups. New reforms are intended to include address a system of equity, accessible and equitable systems of justice for all citizens despite their socio- economic status. Further, there is also a historical approach to managing the limitations built into the laws established by colonial law. The historical colonial system was structured to govern and control the Order, not as a productive system, that engaged the outcome of justice and fairness, as a result the laws lived into anachronistic practices with maintaining colonial sensibilities. The new criminal law reform process acknowledges the built historical challenges, and moves to resolute a more contemporary legislation that has contemporary sensibility. These reforms are important upgrades to the Indian Justice System. And, importantly they

address both the limitation of meeting the needs of a justice processes that are build on a history of colonialism, but they reflect a promised move towards progressive possibility of a just society to the farthest expanding meaning of the word. The historical soaking in the language, by modernising the laws and processes, to not only improve the effectiveness of the justice process systems, or systems of laws to them being more contemporary and voluble by society, and as such missions of service to all citizens will be provided. Ultimately, the modernisation of criminal law represents a progressive change for justice in India, recognising the deep historical context but also grappled with the imperative for change to develop a more appropriate, equitable, and effective justice process.

The Bharatiya Nyaya Sanhita, 2023 aims to reform our criminal code by providing updated definitions of crimes and corresponding punishments. More specifically, it adopts a legislative posture that aims to align the justice system with both modern social mores and proposed changes in technology and communication aspects. In addition, Bharatiya Nyaya Sanhita, 2023 introduces strict guidelines for handling a number of more serious offenses—with a specific focus on protecting the rights of victims of crimes, especially women and children, as well as individuals from marginalized communities, and those who may have been denied access to the justice system due to related conditions. The Act proposes stricter punishment for certain offenses and provides faster trial processes in an attempt to ultimately reduce the convictions of individuals charged with performing some of those acts in the first place by adding to the oppressive aspect of criminal punishment and accountability communities will potential feel in a trust toward the justice system. The Bharatiya Nyaya Sanhita, 2023 signifies a thorough overhaul of India's criminal law, aimed at updating the definitions of crimes and their punishments wherever felt necessary. The code sets out a number of important changes. The Act updates the definitions of different offenses with an eye to contemporary norms in society and new technology. One emphasis is on preventing and suitably assisting victims. Within that remit, special attention is paid to aiding and protecting underrepresented groups, such as women, children, members of marginalized communities and others. There are explicit protections to protect those people during judicial processes and throughout their cases. The Bharatiya Nyaya Sanhita recognizes that length of time spent in legal processes can be a huge barrier for victims in viewing justice occur. Therefore there are provisions enacted to speed up trials, most notably time restrictions on investigations and the process of going to court as a victim, thus compressing the time period a victim is undergoing the process without result. Serious punishments were enacted for serious offenses related to an increased perspective on the growing risk of such offenses, e.g. sex-offenses against children, human trafficking and organized crime. This is intended to deter such offenses, and to demonstrate a perspective and ethos of zero tolerance for the serious offenses.

Bharatiya Nagarik Suraksha Sanhita, 2023 is about citizen security and strengthens police enforcement with the introduction of more advanced technology into policing processes. More accurately, this comprehensive legislation aims to improve not just policing frameworks while addressing policing interaction through the social norms of policing practices—it addresses the investigative process itself, providing enough legislative guidance to fully harmonizing the enforcement agency's administration toward sustained police, citizen engagement, research and publicly engaged prior consent, or presumptuously external via privacy by many individuals and groups. Its stated agenda suggests it is a pledge to provide law enforcement agencies or officers designed processes that clarifies and define their individually sanctioned authority each time, versus opportunistically assume other protections or process ambiguities. The Bharatiya Nagarik Suraksha Sanhita, 2023 aims at augmenting the overall safety of citizens and improving law enforcement efficacy. The law requires the deployment of modern technologies, including surveillance networks, data analytics, and digital forensic technology in policing to further improve investigative capacity and crime prevention. The Act also lays out policies to its already established protocols for law enforcement agencies to improve operational efficiency. This includes training programs for police personnel in policing standards on contemporary investigative techniques and conduct. The Act highlights the need for support services for victims in the investigation process, calls for

independent oversight of police oversight or review of investigative or police misconduct, discusses the establishment of units within departments to deal with sensitive cases, as well as ensuring victims are offered assistance or protection in a timely manner. In current society of deepening wariness of police misconduct, it proposes new measures to ensure greater procedural transparency and accountability, including clarification on how police complaints and police officers must operate independently of police departments.

The Bharatiya Sakshya Adhiniyam, 2023, provides further backing to these changes to the law by reformulating the rules of evidence to promote justice. It is aimed towards improving the gathering of evidence and its presentation and making convictions easier while ensuring the rights of the accused are not violated. The law also includes creative forms of evidence – including digital evidence and forensic developments – that are essential to modern-day crime. It includes provisions to ensure the integrity of evidence and procedure is fair. The Bharatiya Sakshya Adhiniyam, 2023 pertains to standards and processes of evidentiary value with a view to simplify the approach to adduction and to appreciate evidence. This measure revises the practice concerning collection, preservation and presentation concerning evidence. It recognises the increasing relevance of digital evidence by stipulating the process to allow its admissibility in the court system. The proposed measures provide for a fair and just process concerning the evidentiary initiative protecting the constitutional rights to both victims and even the accused. The Act provides protection against evidence tampering and outlines the standards to assess the reliability of witnesses and documents. It provides for the use of sophisticated forensic technologies, such as DNA analysis and electronic surveillance, which is important subsequently to build a better and more reliable evidentiary base - important concerning complex matters or to regulation conviction accuracy. In conjunction, these laws are part of an overall reform to India's criminal justice system. They aim to address problems and gaps in the previous legal framework, advocate for the welfare of victims, and adapt the legal framework to a changing crime landscape in the digital age. By largely focusing on treating and protecting the victim, changing processes to reduce timelines for prosecutions, and utilizing technology, the laws aim to create a more responsive, effective and fair judicial process. Overall, these laws aspire to a legal process and environment that induces a sense of public trust in the criminal justice system, that after the fact, they believe justice was served. By dealing with both traditional and emerging types of crime, the law ensures the relevance and efficacy of the criminal justice system in a world of rapid change.By emphasizing victim protection, speeding up access to justice, and using technology, the reforms have seeked to regain a sense of confidence in the justice system in order for it to be perceived as fair and responsive and capable of delivering justice.These changes in legislation shows a commitment to respect human rights, improve public safety, and create an environment of law where justice is sought and perceived to be done. The enactment of the Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023, and Bharatiya Sakshya Adhiniyam, 2023 is a landmark change in criminal law in India and has raised significant concerns from diverse voice, including NGO’s, academia, legal practitioners and civil rights. Here are some of the primary concerns raised:

The success of these laws hinges on significant upgrades in infrastructure, such as technology and training police in specialized areas of expertise. Without the proper infrastructure and support, the interpretation of these laws may with the greatest of intentions become problematic. There could be added back log if the court system is not prepared for the increased sentencing and expedited trials. Promoting more expedient review must be considered as increased pressure on an already strained system Increasing processing time and numbers will likely burden resources of the jurisdictions. This directly relates to the respect for the trials and the integrity of legal proceedings when the potential for increasing volumes of cases in lieu of speed are processed through any legal system. There will be some potential for police misuse of the powers available to them under these laws, when advanced surveillance and technology is referenced for law enforcement simply "makes sense" but raises further concern over civil liberties and civil affairs, if this is not regulated and constrained appropriately. In regard to the attempt at portraying protection of marginalized communities, I

would prefer to see a bit more wording about protection and disclaiming that perhaps some of systemic bias or discrimination that will at maximum have limited or disparately application with marginalized communities when working with these laws, but it make a fairly big claim by saying all communities. The community perspective on technology and modern forensic methods will naturally eliminate individuals or groups that are already disadvantaged by the ability to access digital tools or procedures in this legal scenario going forward. The Bharatiya Nagarik Suraksha Sanhita, in regard to advanced surveillance and collection of data, makes for serious privacy scrutiny, however, the critics contend privacy in self is being compromised as we create a state of ubiquitous surveillance.

Building on the topics of the reforms discussed above, I have generated a set of potential research questions:
To what extent is the existing infrastructure positioned to accommodate and facilitate the enactments of the Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023, and Bharatiya Sakshya Adhiniyam, 2023?

What effects, if any, will the accelerated trial processes mandated by the new laws have on the existing backlog of outstanding cases in Indian courts? What are the anticipated effects of the reforms on the efficacy of legal processes and the delivery of justice in case of persona data?

What are the possible risks of misuse in connection with the expanded powers that the new laws confer on law enforcement officials?

How might oversight measures be improved to detour potential abuses of power, and connect it to accountability and liability in data breach?

What are the implications for the area of privacy connected with the limited increase in surveillance and data collection in the Bharatiya Nagarik Suraksha Sanhita, 2023?

What to consider with the new laws regarding forensic evidentiary standards and procedural operations, when determining how to develop both?

How effectively does the new reform consider systemic bias and discrimination against already-marginalized populations in digitalization process?

What impacts might the new reforms have on accessibility and fairness in legal processes for marginalized or vulnerable individuals?

Does the reform legislation involve new constitutional or legal ambiguities, if so, how will this impact practice?

How does this area of the reform align with already existing constitutional protections in data violation and privacy?

What will be potential of challenges or benefits faced engaging in forensic evidentiary procedures derived from advanced technology use in law enforcement?

What challenges or benefits could be expected from the implementation of forensic advances under the new laws?

How do India’s new criminal justice reforms engage or factor in learning from international experience with reforms and improving their effectiveness and impact in case of data collection and privacy concerns?

What implications in relation to previous considerations of applying lessons from reform processes could apply as it would to India?

Objectives:
Considering the research questions that have been outlined regarding the Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023, and Bharatiya Sakshya Adhiniyam, 2023 the research objectives are as follows:

To Evaluate the current judicial and law enforcement infrastructure's capacity to effectively implement the new legal frameworks, identifying strengths and gaps.
To Investigate the potential effects of accelerated trial processes on the existing backlog of cases in Indian courts, focusing on efficiency and effectiveness.

To Examine the anticipated effects of the new laws on the efficacy of legal processes and the overall delivery of justice, including the speed and quality of outcomes.

To Explore the risks of misuse associated with expanded law enforcement powers, focusing on potential abuses and the implications for civil liberties. To Propose oversight mechanisms aimed at deterring abuses of power while enhancing accountability in law enforcement under the new laws.

To Investigate the implications for privacy and individual rights related to increased surveillance and data collection under the Bharatiya Nagarik Suraksha Sanhita, 2023.

To Assess the implications of new evidentiary standards and procedural operations, considering how to balance efficiency with fairness.

To Analyze the reforms consider systemic bias and discrimination against marginalized populations, evaluating potential impacts on these communities.

To Investigate how the reforms might affect accessibility and fairness in legal processes, particularly for vulnerable or marginalized individuals.

To Explore any constitutional or legal ambiguities introduced by the reforms and their potential impact on legal practice and interpretation.

To Assess how the new reforms align with existing constitutional protections, ensuring that rights are upheld.

To Investigate the potential challenges and benefits associated with using advanced technology in evidentiary procedures, particularly in law enforcement contexts.

To Evaluate the implications of implementing forensic advances under the new laws, including benefits for investigation and challenges in application.

To Examine how India's reforms engage with international experiences and best practices in criminal justice reform, identifying lessons learned.

To Consider previous reform processes both in India and globally, extracting lessons that can inform the effectiveness and impact of the new laws.

These objectives aim to provide a comprehensive understanding of the implications and effectiveness of the recent reforms in the Indian criminal justice system.

II. LITERATURE REVIEW

The situation regarding Crimes in the country is unfortunately bleak and has shuttered all genuine hopes of the common and learned society regarding possible revitalization of a value based society. The wisdom in the cliché "crime never pays" is dismissed on the basis of hard facts. The malaise of criminalization is impacting on every aspect of social, economic and political activity and there is a steady and accelerated growth in criminality, credibly believed, encouraged by political patronage. The evident and observable criminality appear to be thriving, unchecked and unobserved, notwithstanding the fact that the perpetrators have achieved what they wished without accountability. The apparently acceptable logic of the benign cannon "let hundred guilty go unpunished rather than one innocent be punished" has been distorted by uncommon and unfounded over cautious enforcement, thus incentivising the visible crime and offending criminals to operate freely. The convergence of this conduct, deep rooted criminalization, has created a continuity of a state which vested the administration or pedal power with the criminals and their accessories, is a slippery slope to insecure resource wealth and/or public facility savings of any type.

The society according to K. Sreedhar Rao is greatly troubled and uneasy by the menace of the cyber offenses. Computers and the Internet serve not only as tools for committing crime but target for committing cyber crime. The various types of cyber crime today may include forgery, tampering and fabricating records, mischief i.e. damaging data by cyber means, the offence of criminal intimidation, slander and porno

communication by cyber means to create annoyance are the crimes which can be recognized at this time in the current circumstance. Although the offending conduct shame the above offenses are in chapter XI of the Information Technology Act of 2000 passed by Parliament, the punishments listed under the IT Act seem woefully substandard. The same sort of offending conduct if recorded by the penal laws, even a greater or more severe majority punishment is already prescribed. Therefore, if the infraction punishable under the IT Act are even greater, it follows then punishment structure will have to be determined and prescribed harsher facts (here unreasonable and disproportionate punitive punishments exist) minor sexual abuse by young children often disrupt familial family scores especially of the afflicted, whether juvenile, poor mischief by the act of having forced an adulthood memory from another young juvenile. The basics of the definitions of the offenses contained in the penal laws have to be re-done & added and then reconceived disruptive modifications to match the varied spectrums of the criminality and corresponding punishment must be adjusted proportionate to the circumstances. There has only been a skeletal framework to regulate and supervise networks. Accordingly, significant legislative guidelines must be in place to enforce greater accountability on network operator. For such a system not to be misused for a criminal purpose, the statute should have detailed guidelines and principles incorporated therein. In the present cyber technology it is always possible to fix the identity of the computer from which a criminal activity is done and the place of its location. But it is most difficult to fix the criminal who committed the offence. In the cyber language there is a specific design of language called Internet Protocol Address with the machine address and a originating point of the computer. It is a major and primary evidence in the court. Therefore, in the Act it should be made mandatory for the Internet networks and the computers connected with Internet networks should be maintainable with a licence granted by the competent authorities as has been done in the past, we use to register the radios and transistors as a licence was obtainable to keep a radio. That could easily fix an identity of the customer user of an internet network. If this is made maintainable, a customer user of an internet network web system should also be maintainable. in the present why can we sue the address and information of the customer using internet, the time and the date the Internet as a keeps it as a record and not the message. If it sent and received ok it could be done a secret and not to be given to the network management. After this account of the customer the public through this for the network it could only lead to identify the accused under investigation. The owner of a computer could not be perceive hone, that is the, the owner of a computer connected with the network, could be make the license stands with strict liability. Therefore the remaining parties in indicting the discussion of the offences. And the surveillances of the computer also could be made viciously license a distiches framework would be the ant-fort having at an first and leak able to obit rate the limited misses the networks and nod in identifying. And if practicable cybercrime

There is a steady stream of news reporting about emerging forensic technologies such as DNA typing, data mining, biometric scanning, and electronic location tracking. Supporters praise these forensic technologies for exonerating the wrongly suspected and exposing the shortcomings of a criminal legal system that overly relied on the fallibility of forensic science - handwriting, ballistics analysis and hair and fiber examination. These advocates laud the transition to a "new paradigm" for forensic sciences and are exuberant over the prospects that the newly categorized forensic evidences will forever alter the investigation of, and prosecution of, criminal cases by the government. There is no question that the new forensic sciences will offer the state unassailable levels of certainty and reliability, but these characteristics do not, at face value, mean that they will be less subject to misuse. Indeed, as argued in this discussion, some of the most celebrated characteristics of forensic evidences may very well institutionalize the exact same set of conditions that led to the traditional forensic sciences being discredited. The discussion contends with the new orthodoxy of forensic science; it engages with the memorial and slumbering debate about the role of forensic science in the criminal justice system in three ways. First, the discussion proposes a new taxonomy of forensic evidences that distinguishes first, from second generation forensic sciences. Second, employing the taxonomy, the discussion further emphatically points out how the characteristics of the second generation

forensic science aggravate (rather than relieve) the pathologies that helped to discredit the first generation. Third, the discussion critiques some of the strategies presently being suggested to re-instate the use of forensic science in the criminal justice system that fails to appreciate the specificity of the second generation characteristics, and to suggest alternatives that confront these concerns as specific conditions.

The paper compares responses of Gary Edmond, Joëlle Vuille to incriminating expert evidence (namely, forensic science) from Australia, Switzerland, and the U.S. It begins with an overview of the three systems. It goes on to explain drawing on the recent reviews of the forensic sciences that many of the forensic sciences have simply not been evaluated—that is, have never undergone validation studies. Thus, in many instances, we simply do not know if the technique works, or how well it works. We do not know if the standards, claims of proficiency and experience, and the language methods used by analysts, are based upon empirical studies. These important and troubling findings from across multiple peak scientific entities, and commissions of inquiry (for example, the U.S. National Academy of Sciences and national Institute of Standards and Technology) are used as a vehicle to illuminate on the impact of rules, processes, procedures, and the performance of personnel (for example, forensic scientists, prosecuting counsel, defence counsel and judges) across our three jurisdictions. The paper describes how three different justice systems similarly failed to identify, let alone respond credibly, to structural problems, and endemic, of numerous forms of forensic science and medicine evidences produced and used in criminal investigations by authority and prosecuting agencies. Deep concerns, troubling and serious concerns with forensic science techniques and their derivative evidences hardly if ever, if at all, get noticed, let alone are conveyed, let alone explained for ordinary currency in a criminal trial. Furthermore, there is a challenge establishing clear evidence that lawyers and judges, particularly those in criminal law, keep abreast with the emerging advocacy for critique of the embedding of forensic or speculative expert evidence based on personal, speculative and even irrelevant knowledge, considers to be corrosive when assessing reasonable inferences and proof linking expert opinion to the circumstances of the case and/or a defendant's guilt or innocence. This paper seeks to offer insight into these failures, particularly evidencing, and the weak processes and safeguards we risk across systems of advanced criminal justice, involving adversarial and non-adversarial elements. The appraisals being made of the forensic sciences have been exceptionally harsh. If accepted, the appraisals suggest that some criminal justice systems have troubling and unknown constraints on the credible involvement and regulation of forensic science evidence. The historical inattention of scholars of comparative and other evidence to understanding the value and limitations of forensic sciences has resulted in conversations which tend to be entirely artificial, indeed largely abstract and sterile, because they are conducted around a value for truth above process, human rights, resourcing, the selection, training and experience of counsel, judges and jurors, and the effectiveness of apparent protections such as confrontation, directions of the judiciary and appellate review. Using Australia, Switzerland and the United States as examples, we will argue that apart from being able to suggest improvements in criminal justice, none of those systems have demonstrated an adequate awareness of the problems associated with forensic sciences' uses in routine criminal proceedings practices. They seem unwilling and/or unable to adapt rules and jurisdictional practices that would improve the presentation or evaluation of expert evidence that is incriminating. Our contention is meant to make practices and outcomes more aligned with system aspirations that are above those constraints and the basis of more substantive review.

Erin Murphy discusses New forensic technologies are regularly in the news, from the latest advances in DNA typing, data mining, biometric scanning, and electronic location tracking. How will all this affect the criminal justice system? Many say they will help to identify the guilty. They may also acquit the innocent. An evolutionary shift is now underway, the result of allowing too many unjust convictions to stand for too long. As errors become visible, we recognize the inadequacy of a system once dependent on handwriting analysis, ballistics, hair and fiber comparisons, and similar supposedly scientific methods that have too often played compelling if invalid roles. New forensic technologies offer an unparalleled opportunity to improve the event. From

the advent of most advanced forensic science, myriad possibilities and challenges arise as ways of investigating crime and securing conviction. There is reason to suppose the foundations are about to shift, that we will know more in hitherto unimaginable detail and with a confidence that will greatly influence both investigation and the presentation of evidence in court. There is as well reason to wonder if the new is worth the cost, that we may some day over-rely on technology to ensure justice; that the new technologies may come with invasive shadow effects from data mining to civil robot strikes; or that all the data, noise and certainty may just be something that our lumbering institutions cannot process effectively. That said, there are significant reasons to conclude that forensic science is embarking on a new paradigm.

This Article argues that much of the celebration of these new forms of forensic evidence may only exacerbate the pathologies of the generation of forensic sciences they are supposedly discrediting. A counter-narrative to the dominant story of modern forensic science, this Article intends to politically frame the question of forensic science's place in criminal justice through three avenues. First, it will create a new generic distinction among forensic sciences by creating a typology of first and second generation forensic evidence that will allow us to understand how these generations relate to each other, and how that might in turn relate to the law. Through this demarcation of the generations of forensic evidence, the Article will allow for a more precise and nuanced critique regarding the capabilities and shortcomings of modern forensic science. Second, the Article will not only show why the features of modern forensic sciences--accuracy and precision--trumpeted as virtues are likely to exacerbate the current pathologies of forensic science. The Article will focus on the fact that the seemingly inherent virtue of cutting-edge, responsive, and sensitive modern forensic machinery may lead to rampant and largely shadow evidence against which no one accidentally failing to include human judgment or interpretation is sure. Finally, the Article critiques current approaches to refining the manner and manner in which forensic sciences are used, and the path that second generation forensic sciences present. In doing so, the Article proposes and anticipates alternatives that would provide the solutions that address these problems, as well as the discipline, training, and transparency to show they are viable. In so doing, the Article shows not only that there are social costs in trading one type of forensic for the other, and signals that second generation forensic science might rob us of important political responses.

The Article by JESSICA D. GABEL stresses that forensic shortcomings remain in the criminal justice system and that lapses in forensic science have very serious consequences for justice outcomes (e.g., wrongful convictions and flawed investigatory practices). While there has been increasing awareness of these issues and renewed calls for forensic reform, there is an unparalleled chasm between the yearning for a better system and the reality of moving forward toward that aim. The author emphasizes not reinventing an entirely new system which would be likely extremely costly, but rather utilizing existing structures and frameworks that already exist within the United States forensic science program. The author's point is to promote quality and affordability in forensic practices through collaboration among crime labs, universities, research centers and the criminal justice system to share knowledge of forensic practices, best practices and develop new practices that prioritize reliability and accuracy. The idea of combining knowledge utilizing academic research and objective forensic applications is to create a situation of shared responsibility for best practice and as a result pulling together on additional areas that may continuously improve forensic processes and to assure that emerging scientific knowledge is transferred into day-to-day practice. This Article truly does call for a shift to adequately build a more effective and accountable infrastructure in the forensic science space to reduce the risk associated with tainted evidence while also grasping back to public credibility in the criminal justice system in total. This approach also highlights the notion of shared responsibility towards anything that is better in producing valid results towards justice, wherein reliable forensic science is not solely about the science but more there are principles and values at stake in the legal framework that are essential for justice. This strategy enhances what is currently in place, and therefore optimize quality and cost-effectiveness of forensic practices. The author suggests a collaborative model that creates partnerships among crime laboratories, universities,

research institutes, and others in the criminal justice sector. Collaborative partnerships may push for change, in part from sharing knowledge, bringing state-of-the-art research, as well as rigor and a wider span of effort or process related to best practices in forensic science into practice. For example, while research institutions offer valuable insights and knowledge on scientific design and statistics that adds to the robustness of forensic evidence, crime laboratories provide compelling, targeted expertise to ensure forensic practices translate to practice. Costs and production, thus creating a culture of accountability and continuous improvements to forensic science is possible if there muscles collaboration and concrete sharing of students, exchanges, interactions, and training. This added organizational creativity from these entities, alongside, scientists, can also spurn the development of methods or practices that push reliability and accuracy beyond convention and specific problems of conviction based implementation shortcomings. The article also asserts the value of transparency in forensic science, with strong oversight and data made publicly available to confirm the thresholds for which each forensic practice disciplines its efficacy, tests its weaknesses or limitations in practice, and when and where a method shall yield questionable evidence. Greater open-ness from stakeholders provides. A greater degree of scrutiny for forensic evidence, particularly in a court, to ensure integrity throughout scientific processes of forensic science. In closing, the Article advocates for a joint effort in assiduously building a more efficient, reliable, and responsible forensic science infrastructure to help mitigate the risks involved in flawed evidence and restore public confidence in the criminal justice system as a whole. The Article contains a distinct sense of collective responsibility to serve justice, suggesting that there could exist technical issues associated with forensic science, while also giving importance to reliable forensic science as a valued component to any system of justice which maybe considered honorable or fair. The Article concludes to suggest that we can ambitiously, together foster a more encouraging forensic landscape that can both shed light of past failures but begin to shape a more fair and just future.

Sherry L. Xie cites_Digital Records Forensics is a unique collaborative research project located within the intersection of digital record management, law, and police investigation. The overall aim of the project is to develop a conceptual and methodical approach to evaluate the authenticity of digital records (an aspect of evidentiary production) when they no longer exist in their original, or any other, context to validate their authenticity. The project first undertook a number of comparative studies of peer-reviewed literature in each of these areas, which provided a rigorous conceptual framework that will inform the design and implementation of a number of research methods (law case analysis, case studies, ethnographic studies) that aim to contribute to the emergent field of digital records forensics. The value of this project, is it aims to know the fields, priorities collective advantages, use all complementary strengths of all three fields and offer an integrated approach that works collaboratively to contribute to the validity and reliability of digital records for evidentiary use. In this article, we offer one of our comparative studies, which focuses purposely on the concept of reproduction, as it is understood and acted upon in the digital records management and digital forensics disciplinary spaces. We outline the stark difference in how reproduction is interpreted and enacted in each field, and comment on teh similarities and differences in meaning. We consider the ramifications of this difference to the field of digital records management; chiefly how reproducing records in a digital records space requires goal to develop metadata for their use to work best in authenticity and reliability. In addition to our theoretical contribution, this article serves as a 'timely' pragmatic tool for practitioners working in the field of reproducing digital records; all while adding to the evidence producing process used to reproduce, authenticating and determining the authenticity of digital records. The goal of the initiative is to stimulate interdisciplinary discussion and collaboration for the benefit of practitioners who work in any of the fields. The advent of a discipline labeled digital records forensics, is based upon the above proposed foundation and is intended to scaffold the practice of practitioners in both fields. Digital records forensics aims to integrate the aspects of the records management field focusing on the systematic design and management and preservation of digital records, and with the rigor of the digital forensics arena that focuses on design and collecting and managing digital evidence in a way to preserve the evidentiary nature in a court of law. This article discusses one of the

comparative studies that has examined reproduction in digital records management with the digital forensics field. Our study illustrates the nuanced differences in the interpretations of reproduction in terms of technique and relevance to authenticity and reliability in terms of the fidelity. For example while digital records management may focus on the maintenance of access and preservation of records, the aspect of practice in the field of digital forensics may require higher levels of validation to uphold the evidentiary value or authentication in court. We will explore how these differences can inform each field from the perspective of improving best practices and digital records management in particular. Digital forensics could provide useful considerations in terms of reliability by considering digital records to be reliable. Digital records could become more trustworthy if digital records managers consider issues of integrity and chain of custody as practice protocols for reliable replicated digital documents are created. This is especially useful in a digital world where information is proliferating at a rapid pace and it can be easy to lose the accuracy of original and reliable records. Our respective address also raises the far broader potential implications for practitioners working in legal and investigative spaces, where the truthfulness of some type or other of digital records, such as messages, conversations, and so on will greatly affect the execution of case outcomes. By bringing together those who work in this intersection, we hope to build an explicit understanding of the digital records authenticity, which ultimately enhances the work of practitioners who collaborate with these digital records in their professional practice. Accordingly, the Digital Records Forensics project does not just aim to innovate on two established fields, but it aims to elevate the conversation to improve the practices and principles that we use to assert the integrity and authenticity of digital records, encouraging a collaborative model of digital evidence across legal and investigative spaces.

Orin S. Kerr focuses on the point that The emergence of computers and digital technology has resulted in a radical change to evidence in criminal cases: digital evidence is an abstract entity shaped by binary code or zeros and ones, which exists in the world of electricity and data. In his essay, Professor Kerr analyzes whether the conventional rules of criminal procedure can effectively regulate the collection and analysis of this latest type of evidence. Professor Kerr believes that the typical legal norms pertaining to the collection and use of tangible physical evidence and eyewitness testimony geared to historical understanding of evidence do not fully address the evidence problem with digital or cyber evidence. For example, gathering digital evidence and data collection generally comes with different issues relating to gathering the evidence/data together. The issues of specialized knowledge pertaining to the technical aspects of digital evidence collection, the complexities of digitally stored evidence and data being suspect to tampering, and privacy concerns related to bodily searches of physical evidence are not much of an issue. Kerr suggests current laws concerning gathering physical evidence can deliver unforeseen results by potentially burdening a suspect's rights and, at the same time, ineffectively protect the integrity of the investigation, while a problem exists regarding the burden of data collection. Because of this disconnect, current law needs to be developed and written in such a way to address these issues related to the gathering of digital or cyber evidence which combined reliance on the contemporary norms of law and the informal dimensions of legal evidence. In discussing what these laws would look like, Kerr emphasizes collaboration in developing the new norms in conjunction with legal academics, law officials, and technology specialists to appropriately generate rules of practice that will be both practical and efficient. In sum, Kerr believes institutions should work together to establish a framework which protects constitutional rights, while also relying on the digital and cyber technology facts associated with the digital realm, allowing the investigation to fairly progress through a participation in the sacred nature of justice. Kerr elucidates the points of confusion created by the distinctive characteristics of digital evidence, compared to evidence collected according to traditional rules of evidence. For instance, techniques involved in collecting or recovering and assessing digital evidence often necessitate an amount of technical agility and familiarity with the digital space that many legal practitioners lack. Furthermore, complications introduced by data encryption, the ephemeral quality of information, and the vast amounts of data produced by today's devices add an additional level of complexity that is not sufficiently accounted for by

more traditional methods. Thus, Kerr identifies a number of surprising and concerning implications that emerge when current legal rules are made to fit the collection of digital evidence, including challenges related to privacy rights, potential for overreach in surveillance, and jeopardizing the integrity of the evidence when visibly mishandled. Because of these differences, Professor Kerr makes the compelling case for new legal norms specifically related to the collection and review of digital evidence. In his comments, he suggests establishing the new norms should involve collaboration and input from legal scholars, law enforcement, technologists, and civil rights. Bringing this collaboration together will be necessary for developing a principled system that is constitutionally sound but explicitly demonstrates the realities of digital evidence collection and what programs are needed to protect individual rights. Kerr offers very deep initial thoughts on what these new rules would look like – for example, limits on consent, warrants, and preservation of evidence for pieces of digital evidence, and in turn the digital space must be accounted for.In addition, he points out the foundations of and the need for institutions that will be necessary to establish new rules and standards. These institutions would prioritize taking an educational role for law enforcement, ensuring law enforcement officers have the skills necessary to navigate this changing technology and established educational systems. In conclusion, Kerr's examination illustrates how important it is to recognize the pressing need for legal reform that is responsive to phenomena of technological advancement. Through entering a contemporary discussion on legal infrastructure that takes into consideration the various complexities surrounding digital evidence, Kerr provides an argument for the protection of justice in the face of an overall shift to the digital space, preservation of individual rights against an ever-increasing investigatory base, and upholding norms of due process related to crime commission. This part of the social infrastructure not only seeks to enhance a criminal justice system but wants to maintain that system's relevance in terms of addressing spaces enabled or disrupted from phenomena of advancement in digital technology.

III. LEGAL ANALYSIS

As we now dealing with digital forensic and legal aspect, we now go in deep with that. As technology continues to evolve, Digital Forensics has emerged as a vital and important part of the legal or justice delivery system. Digital Forensic, also known as Computer Forensics. It is an academic area which deals with the procurement, preservation, analyses, and describing digital evidence in the resolution of cyber- crime. This method highlights the active nature of the intersection of digital forensics and legal aspects, and will highlight its relevancy. Digital forensics, or computer forensics, has gained plenty of traction as a key aspect of the legal system and justice in a digital world. As cyber-crime intensifies, the necessity of being cappedable of collecting, preserving, analyzing and interpreting digital evidence has developed into a larger issue of addressing complex matters. The discipline defines a constellation of practice aimed at discovering evidence stored in a digital manner on computers, mobile devices, or stored using the cloud. The legal aspects of digital forensics as a discipline are becoming more meaningful, since the outcome of the investigation could lead to evidentiary process in the legal sphere ranging from a request for a criminal charge to civil litigation. The legal system now accepts digital evidence as reliable evidence, which requires a forensic investigator to follow methodologies and standards of practice to produce reliable and admissible evidence gathered for evidentiary purposes. With the escalation of reliance on digital evidence, understanding the legal issues surrounding the collection and use of digital evidence - related to privacy rights, chain of custody, and breaches of regulations of various types - is a consideration was over shadowed in an initial understanding of the context of digital crime and forensic investigation and prosecution. Additionally, the forensic practice and the legal practice intersection are models that follow the increased ability to adapt, but so do the cybercriminals' utilization, requires digital forensics practitioners to adapt. The practice of digital forensics and the legal practice is a dynamic interaction, provides law enforcement and investigators value and highlight concerns, or issues about ethical considerations very seriously, and apply the requirements to process those rights in the new digital

potential in the practice, of digital evidence gathering and use processes is a dynamic and still theoretical shift in the sphere of action taken to address matters criminal in the digital sphere impact how justice was procurer, adversely has changed.

The central aim of reconfiguring India's legal framework is to design a just and equitable system that meets the expectations of the digital age while tackling the diverse needs of the society. As technology develops, the legal principles governing our relationships and protecting our rights must also evolve. This begs a full comprehension of the particular changes being made and their wide-ranging consequences as these changes will transformative the judicial landscape in the country of India. Which areas are most transformative is redefining evidence and investigation techniques which includes digital footprints and electronic communications as evidentiary components. This new landscape will increase the capacity of law enforcement agencies to intervene between crime initiated digitally and reduce damage and threats made against ordinary citizens. Additionally, the evolution of the scope of criminality expands into new realms due to technological advancements occurring daily, such as data breaches and online stalking. Criminalizing people's behavior is imperative to public safety as we try to also protect people's rights in an increasingly connected world. Embracing the reform changes will lead to a stronger, more efficient, and fair legal system to better serve all Indian citizens, during an age surely in need of fairness, justice, and equity.

Across various legal systems around the world, judiciary bodies are confined to jurisdictional limits, which means that courts may only hear cases that fall within a particular geographic jurisdiction and legal framework. This principle presents serious issues in the domain of computer forensics and there are clearer boundaries for cybercrime, where the scope of digital evidence may breach proper jurisdictional domain. For example, the jurisdiction affording the cyber-criminal will clearly diverge from where the evidence they manipulate, data or physical evidence, is located. The data must fall under the legal process governing the evidences and appropriate use in whatever jurisdiction the case is being adjudicated to be lawful.

This creates a massive problem, as it risks the significant issue of accountability. What is a cybercrime in one jurisdiction may not be a cybercrime in another jurisdiction, creating significant ambiguity. For example, unauthorized data access or hacking may be considered serious crimes that receive harsh punishment in one county, while another jurisdiction may not even classify the same actions as an offense or afford them significant legal restrictions or attention. Cyber-criminals will exploit Europe or even global jurisdictional dispute and punishment as incentive to engage in other forum shopping if their actions or even lack of jurisdiction are not prosecuted or restricted. In addition, these constraints can be taken far beyond just the legal criteria and implications of cybercrime if you expand into the technology space, where legal regimes often lag behind rapid technology advancements in defining and regulating instances of cybercrime. In an interconnected and global society, the lack of uniformity surrounding laws governing rights for digital offenses further complicates the ability of justice or fairness to occur in a uniform manner. This is likely to become more extreme as technology continues to advance and there is much debate over the universal standards of behavior or rights across jurisdictional boundaries. Further, there is an imperative need to balance these issues by bringing the law into greater harmony and collaboration between jurisdictional agencies globally to create clear guidance on how to treat and use alleged attacks for purposes associated with states obtaining justice as to use on digital evidence.

Digital forensics is a field that is changing rapidly. While digital forensics serves a critical purpose in the context of investigating cyber crimes, it faces numerous serious challenges that need to be addressed to enhance its usefulness.

Technological Changes: Technology is always shifting, with new hardware, new software applications, new behaviors, and new data encryption methods constantly appearing. Digital forensic methodologies must adapt to the changing array of devices and applications to assist with accessing or analyzing collected evidence from these novel environments. An example is mobile devices that employ encryption preventing access to information. Also, data residing in the cloud has also exploded in

proliferation, adding another layer of complexity for investigators, and with data being stored across multiple jurisdictions, forensic professionals must also consider the legalities across these jurisdictions as well. Therefore, with the constant advancement of technology, it is imperative for forensic professionals to leverage the latest technological advances and create new methods to meet these challenges.

Privacy Considerations: Whether the requirements for law enforcement and the privacy of the individual under-criminal investigation are at odds with one another is a "hot" topic within the digital forensics community. Law enforcement investigators are often attempting to access digital evidence that may be incriminating and yet be operating within a legal framework designed to protect the privacy of a citizen. There exists a philosophical struggle over the appropriate means to collect digital evidence without infringing upon an individual's protected right to privacy. Law enforcement is bounded by standards of conduct and ethical practices to conduct a lawful investigation which may limit their ability to act quickly and responsibly throughout an investigation. Balancing the individual or citizen's right to privacy and the need for law enforcement to conduct an investigation onto criminal behavior is of utmost importance not only to garner confidence in public trust, but also the gathering of evidence for legal use should the need arise. The greater good may require change, possibly requiring thoughtful participation between attorneys, technologists and advocates for civil rights, to curate processes that balance privacy consideration while equipping law enforcement to conduct investigations.

As cybercrime investigations must become stricter, privacy issues and data breaches will require thoroughness as well. Therefore, federal law enforcement must adopt a balance between effective law enforcement and safeguarding personal and national data security. In cyber cases, it is no secret that law enforcement would face challenges in finding evidence that does not interfere with citizens' privacy rights. For instance, the tools utilized to acquire evidence include more sophisticated weapons such as data mining and deep packet inspection, which can lead to the capture of numerous personal information from individuals. No matter how these pieces of personal information contribute to the issue or the suspect, the very act of capturing and using these sensitive personal and privacy information obtained doubtless raises enormous, and morally challenging concerns in the realm of digital information. The suit of these personal information is subject to ethical and legally sensitive requirements on how these data should be maintained, archived, and used and shared under which data mining technology will get only the necessary sensitivity, and the liability of data breach may be increased, and any slight error would be the loss to the wrong hand or abuse. To sum up, privacy rights must receive new enforcers to ensure that private data is properly collected, archived, and used. Strict guidelines to maintain privacy rights should be established and performed by local state and federal law enforcement agencies. Moreover, as long as law enforcement agencies engage in criminal investigations in a transparent, legal manner, public trust and confidence in law enforcement activities will increase. Policymakers, technologists and activists should be suggested to legislate and make a solid foundation to find out the real risks of cyber power through open dialogue because treated as such awareness. It should be mentioned that the regulatory framework should not simply protect the recognized information privacy rights of individuals through open dialogue, or protect US national data against illegal intrusions, but also allow institutions to collect and use individual Internet data, the sensitive information and between countries. Additionally, investing in advanced training for investigators can enhance their understanding of privacy implications and the importance of ethical data handling. By equipping law enforcement professionals with the knowledge and tools to navigate the complexities of digital evidence, we can create a more responsible investigative environment that honors both security and individual privacy. Ultimately, striking this balance is essential for fostering a safe digital landscape that respects personal rights while empowering law enforcement to effectively combat cybercrime. Achieving this equilibrium will require a concerted effort from all stakeholders involved to ensure that the investigation processes are not only efficient but also ethical and secure.

Training and Knowledge: Given the ongoing demand for proficient digital forensic practitioners, law

enforcement organizations and legal practices must confront the impending issues regarding their investment in training and technology. The digitization of evidence raises questions regarding the necessity of a specialized combination of knowledge in the fields of computing, investigative procedures, and legal standards. Aside from the evolving technology surrounding forensics, without trained individuals, opportunities for mishandling evidence and/or misinterpreting data, would increase and consequently risk prolonging investigations and/or jeopardizing any related legal proceedings. Moreover, professional engagement with specialized cyber training and/or institutional capacity building have significant value, because these professionals must necessarily update their skills consistently or face the persistent cyber threats of new technology. When agencies invest in training and technology, they can adequately professionally adapt and anticipate the continual evolving threat of digital forensics in today's cyberspace. Meeting these needs is crucial for the future of digital forensics practice, because this issue impacts more than just the effectiveness of investigations, it also spills over into the way the public perceives law enforcement can simultaneously protect security and individual rights.

To progress with the examination of the evidence in court, it is required that the forensic investigating officer establish their credentials in order to substantiate their expertise as well as the reliability of the evidence provided. In order to prove this experience, they may need to qualify as to the education they have obtained, the number of investigations in which they conducted procedures a such investigator, the tools that were utilized to acquire or analyze evidence, and the steps taken to be able to present the evidence in court. The forensic investigator must ensure validity and integrity, which is accomplished by producing a bit stream copy of the original media using a forensic software. The original media should not be analyzed under any circumstances, given that this media will be presented as an exhibit in court or if the opposing side challenges what is discovered. The mirror image is used as a means of preserving the evidentiary value of the information recovered; although there is still risk for the digital media to be altered, a proper forensic process will uncover that change.

Digital evidence is inherently fragile and typically loses its worth unless collected, protected, and safeguarded conservatively and in a timely manner. It can easily be deleted or altered with just the click of a mouse. Thus, preserving evidence is an important function of the investigation process from the outset. The investigating officer must establish through testimony in court that the evidence has not been altered in any way and therefore the evidence can be trusted to be truthful in order to establish admissibility. The chain of custody supports that the evidence has not been altered in any way by documenting how evidence has been collected, preserved, analyzed and eventually entered into the court of law. A strong chain of custody establishes that the digital evidence can be trusted. In many jurisdictions, existing legal approaches are extremely insufficient as the investigators do not have the training and technical skills to preserve digital evidence as chain of custody into litigation. Many perceived electronic discovery processes and technologies are seen to be too costly and legal processes mostly are only addressing preservation of manual paper documents or letter correspondence.

Dow Jones & Company Inc v. Gutnick stood as an important case in the field of defamation law, especially with the issue of online publishing and jurisdiction at hand. The case came about in 2002 when an Australian businessman, Joseph Gutnick, filed suit against Dow Jones & Company, who was the publisher of the Wall Street Journal, for defamation. The controversy arose after an article was published online on the Wall Street Journal website alleging that Gutnick had involved himself in deprivation. Thus, the legal issue arose to whether an Australian court could have jurisdiction over Dow Jones, a company located in the U.S., since the article was published online and accessed by readers in Australia. Gutnick alleged that the damage from the article occurred in Australia, which may allow the local court to assert jurisdiction. The High Court of Australia determined that Dow Jones could be sued in that jurisdiction. The court stated that defamation occurs where the material is published, and said that place is where the affected individual lives. Thus, since the article was published and accessed in Australia adversely affecting Gutnick's reputation, jurisdiction would be established. This case is significant due to the

implications surrounding internet defamation and the defamation risks that an online publisher may be subject to, based on the jurisdictions that it may receive viewing and attention. The case made it more apparent that an internet publisher could be subject to defamation law in a number of different jurisdictions based on where the viewing occurred and the and the resulting effects. Ultimately, Dow Jones & Company Inc v. Gutnick is a foundational case that has changed the nature of defamation and how jurisdiction operates in relation to our case, especially when considering issues involving international law and content available for viewing online.

Preservation and storage of evidence an important issue In the case of Weiller v. New York Life Insurance Company, the court began to address preservation issues arising out of a dispute over an insurance claim. The court ordered New York Life to preserve electronic documents, but the defendant claimed that it would be expensive to preservation. The trial court ruled that New York Life's existing federal preservation orders did not adequately protect the interests of the plaintiff. Ultimately, this decision highlighted the obligation of parties to litigation to preserve materials and documents that are reasonably believed to be relevant to the case during the time period of the litigation, especially electronic documents and information, to prevent spoliation and a duly process otherwise needed for the trial. The ruling reinforced the role of the court to review, replace, and protect the evidentiary process.

Document destruction is a widespread practice in both individual and business population in the course of their natural business undertaking. If you do not have an effective e-discovery policy, it can interfere with preserving valuable data and Electronically Stored Information (ESI). Without knowing what records need to be preserved and when, employees may inadvertently delete or modify vital data, which can increase the risk of complications in the event of litigation. More important still, both parties to a lawsuit are required to produce all relevant documents to the other party. Therefore, careless or intentional deletion or modification of evidence can create additional legal problems and affect the ability of the party concerned to comply with their discovery obligations. Moreover, the court system needs time to adapt to the unique aspects of ESI. Although e-discovery is routine in many courts, there are a significant number of courts that are hesitant to embrace it. Courts may view ESI as less important than paper records when they are skeptical of electronic data discovery. The reasons for this concern are numerous and include the potential for massive volumes of ESI and its technical and possibly incomprehensible nature. As a result, not all courts handle electronic evidence in the same way, and adding to the complexity, discovering or proving your case. In addition, not all courts treat ESI equally, and its addition to the legal system may be inconsistent and difficult. To amend this, corporations should set up robust e-discovery policies and procedures in order to maintain, preserve, and manage data. Every employee should be well-versed in the requirements for preserving ESI, and a procedure should be in place to initiate a litigation hold. Moreover, courts should not resist recognizing the importance of electronic evidence and need to set procedural guidelines for clarifications. By promoting proactive data handling and expanding the courts' comprehension of the complexities of ESI more, both businesses and the Court system, can better manage data.

The case of Galaxy Computer Services Inc. v. Baker dealt with the issue of whether an expert in computer forensics could testify about the analysis he performed in the case when the defendant challenged the expert's qualifications. The issue raised by the defendant was largely related to the expert's educational background and methods and whether that could form the basis of the reliability of the expert's findings. The court found that the expert had a firm educational foundation in computer sciences and forensic analysis, along with reasonable collateral experience in the area of computer forensics, including being employed by a law enforcement agency to conduct forensic investigations. The court noted that the expert was able to demonstrate that he used the appropriate processes and tools, which were fundamental to upholding the reliability of his findings. In the end, therefore, the court concluded that the expert had sufficient qualifications and that the methods he used, were reliable enough to meet the legal standard for admissibility. This finding illustrates the judicial system's trend towards recognizing that emerging disciplines such as computer forensics cannot always

be measure by traditional qualifications of experts, and as such, a decision of admissibility could merit qualification by practice, grounded experience and demonstrated skills of the expert. This determination of testimony was found to be influential in developing the concept that practical experience could follow an individual through their community rather than formal qualifications being the only predictors of expertise to determine if the testimony should be viewed as valid and reliable in a court of law.

In numerous jurisdictions, there still exists an absence of laws or regulations governing expert qualifications, and the question subsequently arises regarding consideration of someone as expert because of the ability to use forensic software tool.

Braintech Inc. v. Kostiuk was a decision of the Supreme Court of Canada that looked at jurisdiction for matters arising from internet-related activities and its implication for jurisdictional disputes. In this case, Braintech, a company located in British Columbia, was seeking to bring a proceeding in Texas against Kostiuk, who resided in Canada. The main issue was whether Texas could exercise jurisdiction over Kostiuk, and in order to make this determination, the question was whether Kostiuk, merely by accessing information on the internet, was subjecting himself to the jurisdiction of the Texas court. The courts made a finding that there were no valid jurisdictional grounds based solely on Kostiuk's access to information on the internet. The court recognized the basic principle of sovereignty wherein a court in one country cannot freely exert its jurisdiction over a resident of another country without clear substantive contacts to the jurisdiction. In this case, the Texas court did not have jurisdiction to hear the lawsuit as Kostiuk did not have sufficient contacts with Texas. The ruling illustrated the limitations of traditional concepts of jurisdiction, particularly in the face of widespread geographic implications of the internet and online communication. The Supreme Court further highlighted the fact that courts are compelled to scrutinize the nature and quality of the contacts that the Defendant has to that jurisdiction before determining that a court can assert jurisdiction. The case continues forward to set important ramifications for the future litigation of internet-based activities and that operating in the virtual world does not mean jurisdictional authority exists. In conclusion, Braintech v. Kostiuk addresses and demonstrates the challenges courts face in navigating jurisdiction within matters related to the internet and the need to maintain the sovereignty of legal systems in an increasingly connected world.

In the case of State (NCT of Delhi) v. Navjot Sandhu (2005), the Supreme Court of India evaluated electronic records as admissible evidence within the confines of the Indian Evidence Act. The Court stated that electronic records were admissible without a certificate from any person at all under Section 65B(4) of the Act and emphasized the need to safeguard the evidentiary value of electronic documents from being destroyed and undermined by procedural niceties. This case demonstrated the importance of allowing electronic evidence to be considered for purposes of ensuring that justice was accomplished if the electronic record possessed certain characteristics of reliability and authenticity. This case was a significant step in recognizing the role of evidence in the digital era and establishing precedent for electronic records.

CONCLUSION

The establishment of the BNSS (Bharatiya Nagrik Suraksha Sanrakshan) represents a significant turning point in India's efforts to incorporate digital forensics into its criminal justice system and conveys an increasing recognition of the impact of technology on contemporary law enforcement. The BNSS legislation acknowledges the importance of audio-visual evidence and creates appropriate frameworks at the police level for its acquisition, storage, and presentation as evidence in court. The BNSS, which is critical to the integrity of evidence necessary for the administration of justice in a digital age, regulates audio-visual evidence to prevent distortions or misrepresentation, while establishing guidelines in a more streamlined manner for the investigation of cybercrimes, while these crimes have proliferated alongside the rise of technology in our daily lives. However, to fully maximize the transformation potential of digital forensics, a number of issues must be considered. The first issue which must be addressed for capacity building for law enforcement professionals is the need for training at the level of skilled employees who are knowledgeable in the latest forensic technologies. Forensic methodologies are not

only technical; those trained must also be aware of criminal and administrative law considerations, or the overlap of technology law into criminal law may lead individuals astray. Next, law enforcement and criminal justice systems must be supported with additional tools and digital evidence related infrastructure, to advance beyond a reactionary approach to technology and forensics. Legal experts and technology specialists can specifically contribute needs assessments towards investment in best practices and technology innovations in select cities with a favorable environment to do so. Public information and education about digital rights, as well as the implications of digital evidence, must also be considered, as citizens need to understand their rights and responsibilities as members of this evolving criminal justice system. Finally, the investigation must estimate the potential need for periodic reviews of the BNSS as well, as technology and cybercrime evolve. To the extent possible, the public functions of government may also require increased scrutiny related to their evolution in to and within this criminal justice system with technology and digital evidence.

First and foremost, it is imperative that law enforcement officers, attorneys and the general public have an increased understanding of digital forensics and its unique role in our legal system, as understanding the complicated nature of digital evidence can often serve as an obstacle in both investigations and in a courtroom. Educational opportunities in digital forensics, and training programs, will help demystify the complicated nature of digital evidence and prepare participants with knowledge to interpret and act on forensic evidence. Tailored workshops, online courses, and the general public can become educated through outreach provided to law enforcement officers, explaining how this knowledge will allow them to collect, process, and examine digital evidence in a manner that conforms to legal obligations. On the attorney side, educational training will enhance their understanding of digital forensics, so they can present evidence in court in a more effective manner while advocating for their client's rights and professionalism. For educational awareness for the general public, it is important to develop programming for education around digital forensics principles. The public must be educated about their rights, data privacy implications, and the implications of existing evidence in digital contexts. Simultaneously, there is also a need for increased collaboration between law enforcement agencies, business leaders, and educational institutions to innovate, improve the research agenda, and prepare digital forensic skills. Sharing, collaborating, and innovating together will result in knowledge sharing and a body of experience that can facilitate the development of best practices in this emerging field of study. For example, academic institutions may provide research or thought leadership to law enforcement agencies to ensure they are not left behind during continuous advancements in technology that create increased potential threats for law enforcement officers. Moreover, collaboration can also bridge the gap between real-world application and theoretical knowledge, as businesses may offer observational opportunities and advice. Finally, a collaborative, unique initiative could develop internship programs as students prepare to enter the workforce. Internships can provide work to their respective educational institutions as they allow for student engagement, regardless of the agency location. An efficient collaborative ecosystem can also foster the establishment of standardized protocols and methodologies, promoting consistency and reliability in forensic processes across jurisdictions. This will likely result in a much better informed community that understands and appreciates the contribution and value of digital forensics to various law enforcement efforts. This knowledge will lead to a more effective investigation, stronger arguments in legal proceedings, and ultimately a justice system that is able to address the demands of the digital age. In short, by investing in education and collaborating, stakeholders can develop a sustainable collaborative model that serves not only to improve the capacity of individuals in the justice system but also improves the integrity and efficacy of the justice system as a whole.

In addition, given the inherently transnational character of cybercrime, effective international cooperation forms a key ingredient for effective evidence gathering and proceeding against offenders. Cybercriminals often operate across borders and exploit legal and jurisdictional loopholes, impacting law enforcement and investigations and delaying criminal justice. As a first step, India must advance negotiations for various strong bilateral and multilateral agreements with other countries that make

mutual gathering of evidence and exchanging evidence possible, secure and timely. Agreements could include arrangements for mutual legal assistance, expedited extradition, and protocols for sharing digital evidence securely. This can include conversations about mutual understandings and engagement with INTERPOL and the United Nations, assuring alignment on INTERPOL and United Nations standards and cooperation on cybercrime matters. Shared collaboration can also include joint exercises to forge capacity, share information, and develop common standards or best practices around digital forensics available to other countries. Cumulatively, a global approach improves the capacity of Indian law enforcement and creates networks of allies that will combat cybercrime. By tackling these matters in a comprehensive manner, India would perceive itself as a decision-maker in the digital forensics field and would no longer be standing on the sidelines or observer. The need for leadership in this rapidly changing world is important. We cannot ignore as wrestlers in a world of increasing and numerous cyber-risks, that we must continually seek new paradigms and innovative answers. Alongside investment into education, continuing collaboration across India and other countries in the G20, digital forensics paired with law enforcement must become one of the pillars of the legal system - supporting law enforcement, justice, and protecting citizens in an ever-changing and at times adversarial - digital world. This pillar is developed with law enforcement focused units on cybercrime and/or digital forensics, legal frameworks aimed at keeping pace with technological innovations, and a commitment (in all respects) to ongoing iteration and learning. Therefore, India can adopt these responses into their legal frameworks and law enforcement processes to increase the rule of law, develop public confidence in the legal system and respond to the challenges posed by the rapid growth of cousin and digital crime; creating a safer and more secure future in the digital world.

Investigators encounter significant legal considerations that require careful consideration to safeguard the admissibility and integrity of digital evidence. The processes behind the collection, storage, and presentation of digital evidence are bound by a complicated legal framework, and investigators' actions and procedures must adhere to these legal guidelines. Failure to obey the legal frameworks could seriously limit the admissibility and integrity of evidence and disrupt and halt the prosecution's efforts and the case itself, in other words. For instance, if investigators do not take due care in the manner in which they acquire digital evidence—for instance, following the chain of custody, obtaining proper and necessary warrants, or do not comply with any outside legal statutes—they could risk the court considering the evidence inadmissible. This would cause severe gaps in the case, and allow even a guilty party to go without consequences. Further, failure to follow proper procedures surrounding digital evidence could expose investigators and their department to liability in countersuits, particularly when individuals believe their rights were violated during an investigation. Police liability could stem from claims for invasion of privacy, unlawful search and seizure, or violations of laws or legal representation. Additionally, even when individuals are not seeking liability through a countersuit, negligence and illegal actions can be damaging to a department's reputation with the public and damage trust in law enforcement as a whole. This reality can be detrimental to law enforcement designs, and in turn make investigations much more difficult further on. Given the complexities of the law, it is vital that investigators receive a thorough understanding of the legal aspects of digital forensics, so that they are aware of the laws associated with their actions in addition to the digital forensic processes. Through compliance with the legal framework, investigators can ensure the admissibility of evidence, such as digital and electronic evidence, protect themselves from truthful consequences of law, and protect and serve the integrity of the respective jurisdictions. The BNSS's implementation is posed to provide a multitude of critical benefits and servitudes that may significantly change the complexion of investigations dealing with cybercrime. Besides forming a robust legal framework for the proper collection and use of digital forensic evidence, the BNSS enhances the efficacy of law enforcement agencies to fully investigate cybercrime-related cases and also raises the probability of successful prosecutorial outcomes. Digital forensic evidence generally comprises data extracted from electronic devices. By this, extensive investigative processes can be made a lot easier, thus saving precious man-hours and resources that would otherwise have been used by law enforcement

agencies in their more traditionally used modes of conducting an investigation. Besides, the setting-up of clear guidelines that specify the practices involving chain of custody for digital evidence ensures that this evidence has a higher probability of being admitted in court, which subsequently helps the integrity of the judicial process.

However, the legislation has also had its own share of hurdles. Experts in law, law enforcement officers, and the general public must, thus, be thoroughly trained on the niceties of the BNSS provisions and their application with digital forensics. This will help to ensure the understanding of the provisions so as to implement them successfully and maximize their effectiveness. Further, the establishment of adequately upgraded digital forensic laboratories and personnel qualified with the required skills is also an important step in the implementation of the BNSS. Then, within the great tension that exists between effective investigations and the need to protect personal data and privacy, it remains an encumbering proposition. Finding that balance very much remains a challenge as the administration of justice cannot be at the detriment of an individual's rights. These complexities will require ongoing dialogue among stakeholders, comprehensive training programs, and adherence to ethical standards that uphold privacy protections along with public safety.

REFERENCES

[1] Murphy, E. (2007). The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence. *California Law Review*, *95*(3), 721–797. Accessed 20 Sept. 2024. http://www.jstor.org/stable/20439109

[2] Rao, K. S. (2001). CRIMINAL JUSTICE SYSTEM — REQUIRED REFORMS. *Journal of the Indian Law Institute*, *43*(2), 155–173. Accessed 20 Sept. 2024 http://www.jstor.org/stable/43951765

[3] Mirjan R. DamaSka, The FACES OF JUSTICE AND STATE AUTHORITY: A Comparative Approach to the Legal Process (1986) (describing the Anglo-American and Continental legal procedures as adversarial and "nonadversarial, respectively)

[4] JOHN D. JACKSON & Sarah J. Summers, The Internationalisation of Criminal Evidence (2012) (conducting a comparative study on evidence laws across international borders).

[5] Matthew T. King, Security, Scale, Form, and Function: The Search for Truth and the Exclusion of Evidence in Adversarial and Inquisitorial Justice Systems, 12 INT'L LEGAL PERSP. 185 (2002)

[6] Rudolf B. Schlesinger, Comparative Criminal Procedure: A Plea for Utilizing Foreign Experience, 26 Buff. L. Rev. 361 (1976)

[7] James Q. Whitman, Equality in Criminal Law: The Two Divergent Western Roads, 1 J. LEGAL Analysis 119 (2009).

[8] Peter Alldridge, Scientific Expertise and Comparative Criminal Procedure, 3 INT'L J. ON EVIDENCE & PROOF 141 (1999)

[9] Dan L. Burk, When Scientists Act Like Lawyers: The Problem of Adversary Science, 33 JURIMETRICS J. 363 (1993)

[10] Anthony Champagne et al., Are Court-Appointed Experts the Solution to the Problems of Expert Testimony?, 84 JUDICATURE 178 (2001)

[11] Sophia Cope, Ripe for Revision: A Critique of Federal Rule of Evidence 706 and the Use of Court-Appointed Experts, 39 GÖNZ. L. Rev. 163 (2003)

[12] Geoffrey L. Davies, Court Appointed Experts, 23 Civ. Just. Q. 367 (2004) (U.K.)

[13] Ellen E. Deason, Court-Appointed Expert Witnesses: Scientific Positivism Meets Bias and Deference, 77 OR. L. REV. 59 (1998)

[14] Edward V. Di Lello, Note, Fighting Fire with Firefighters: A Proposal for Expert Judges at the Trial Level, 93 COLUM. L. Rev. 473 (1993)

[15] Ho Hock Lai, A Philosophy of Evidence Law: Justice in the Search for TRUTH (2008) (describing the philosphical underpinnings of evidentiary rules and procedures).

[16] GABEL, J. D. (2014). REALIZING RELIABILITY IN FORENSIC SCIENCE FROM THE GROUND UP. *The Journal of Criminal Law and Criminology (1973-)*, *104*(2), 283–352. http://www.jstor.org/stable/44113391

[17] Reddy, A. R. (2009). FROM JURISPRUDENCE TO JURIMETRICS: A CRITICAL EVALUATION OF THE EMERGING TOOLS

IN THE JUDICIAL PROCESS. *Journal of the Indian Law Institute*, *51*(1), 92–101. http://www.jstor.org/stable/43953427

[18] Bellasio, J., Silfversten, E., Leverett, E., Knack, A., Quimbre, F., Blondes, E. L., Favaro, M., & Paoli, G. P. (2020). *How could technological developments influence the future of cybercrime?* RAND Corporation. http://www.jstor.org/stable/resrep27753

[19] O Angelopoulou and S Vidalis, An Academic Approach to Digital Forensics ,Journal of Information Warfare Vol. 13, No. 4 (2014), pp. 57-69 (13 pages) Armistead TEC LLC https://www.jstor.org/stable/26487467

[20] Xie, S. L. (2011). Building Foundations for Digital Records Forensics: A Comparative Study of the Concept of Reproduction in Digital Records Management and Digital Forensics. *The American Archivist*, *74*(2), 576–599. http://www.jstor.org/stable/23079051

[21] Luciana Duranti, "From Digital Diplomatics to Digital Records Forensics," Archivana 68 (2009): 39–66

[22] Richard Pearce-Moses, A Glossary of Archival and Records Terminology http://www.archivists.org/glossary/term_details.asp?DefinitionKey=1584, accessed 20 December 2024

[23] Luciana Duranti and Randy Preston, eds., International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records (2008), InterPARES 2 Project, "InterPARES Book," http://www.interpares.org/ip2/book.cfm, accessed 20 December 2010, in particular, "Chain of Preservation," 195

[24] Brian Neil Levine and Marc Liberatore, "DEX: Digital Evidence Provenance Supporting Reproducibility and Comparison," Digital Investigation 6, Supplement 1 (2009): S48–S56

[25] Albert J. Marcella and Doug Menendez, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2nd ed. (Boca Raton, Fla.: Auerbach Publications, 2008)

[26] Anthony Reyes, Cyber Crime Investigations—Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors (Rockland, Mass.: Syngress Publishing, 2007)

[27] Karen Kent et al., "Guide to Integrating Forensic Techniques into Incident Response SP800-86" (2006), National Institute of Standards and Technology (NIST), Department of Commerce, http:// csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf, accessed 3 August 2010

[28] Marcella and Menendez, CyberForensics. An image is "An accurate digital representation of all data contained on a digital storage device." National Institute of Justice, Department of Justice, Forensic Examination of Digital Evidence: A Guide for Law Enforcement (2004), http://www.ncjrs.gov/pdffilesl/nij/199408.pdf, accessed 1 August 2010

[29] DoD5015.2 Electronic Records Management Software Applications Design Criteria Standard," Department of Defense (2007), http://www.dtic.mil/whs/directives/corres/pdf/501502std.pdf, accessed 16 April 2010

[30] Garfinkel, Simson L. "Digital Forensics." *American Scientist*, vol. 101, no. 5, 2013, pp. 370–77. *JSTOR*, http://www.jstor.org/stable/43707091. Accessed 25 Sept. 2024.

[31] Feldstein, Steven, and Brian Kot. "Digital Forensics: Different Tools, Similar Outcomes." *Why Does the Global Spyware Industry Continue to Thrive?: Trends, Explanations, and Responses*, Carnegie Endowment for International Peace, 2023, pp. 11–12. *JSTOR*, http://www.jstor.org/stable/resrep48430.7. Accessed 25 Sept. 2024.

[32] Kloosterman, Ate, et al. "The Interface between Forensic Science and Technology: How Technology Could Cause a Paradigm Shift in the Role of Forensic Institutes in the Criminal Justice System." *Philosophical Transactions: Biological Sciences*, vol. 370, no. 1674, 2015, pp. 1–10. *JSTOR*, http://www.jstor.org/stable/24505157. Accessed 25 Sept. 2024.

[33] Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. In *Digital Evidence and the U.S. Criminal Justice System: Identifying*

Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence (pp. 1–32). RAND Corporation. http://www.jstor.org/stable/10.7249/j.ctt15sk8v3.1

[34] Orin S. Kerr. (2005). Digital Evidence and the New Criminal Procedure. *Columbia Law Review*, *105*(1), 279–318. http://www.jstor.org/stable/4099310

[35] Kacha Janki, Digital Forensics Legal Aspects, Nyayags Society of Forensics and Criminal Justice , https://nyayags.org/digital-forensics-and-legal-aspects/

[36] George Raburu, Lawrence Dinga , Legal Issues in Computer Forensics and Digital Evidence Admissibility, IJCSMC, Vol. 9, Issue. 7, July 2020, pg.86 – 89 , https://ijcsmc.com/docs/papers/July2020/V9I702021.pdf

[37] ANGELA, B., & RODGER, J. (2005). Identification of legal issues for computer forensics. Information Systems Management. Accessed 03 January 2018.

[38] JAMES,T., & PATRICIA, A.H. (2008). Digital forensics and the legal system: A dilemma of our times. Edith Cowan University, Research Online http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1040&context=adf Accessed 03 January 2018.

[39] Dow Jones & Co Inc v Gutnick [2002] HCA 56; 210 CLR 575; 77 ALJR 255; 194 ALR 433

[40] Weiller v. New York Life Ins. Co., 2005 N.Y. Slip Op. 50341 (N.Y. Sup. Ct. 2005)

[41] Galaxy Computer Services, Inc. v. Baker, 325 B.R. 544 (E.D. Va. 2005)

[42] Braintech Inc. v. Kostiuk (1999), 120 B.C.A.C. 1 (CA);. 196 W.A.C. 1.