PIONEER
ACADEMIC PUBLISHING LIMITED

Studies in **Law and Justice**

Volume 4, Number 3 **June 2025**

CONTENTS

PIONEER
ACADEMIC PUBLISHING LIMITED

Studies in Law and Justice
ISSN 2958-0382
www.pioneerpublisher.com/slj
Volume 4 Number 3 June 2025

When Algorithms Testify: Addressing the Explainability Gap of AI Evidence in Criminal Cases

Yuxin Chen[1]

[1] Law School, Beijing Normal University, Beijing, China
Correspondence: Yuxin Chen, Law School, Beijing Normal University, Beijing, China.

doi:10.56397/SLJ.2025.06.01

Abstract

The expansion of generative artificial intelligence evidence in the field of criminal justice has exposed the structural risks caused by the unexplainability of algorithms. Although existing studies have revealed multiple obstacles, they have not yet touched upon the fundamental crux of the unexplainability of the algorithm. The three predicaments derived from this, namely the disruption of argumentative logic, the loss of focus in the cross-examination process, and the depletion of judicial trust, essentially stem from the subtle tension between the certainty of machine conclusions and their mystery. The solution lies in establishing a transparent evidence generation mechanism, introducing an expert-assisted review system, and setting up traceability rules for training datasets. Through certain system, a dynamic balance is achieved between technological empowerment and procedural justice to prevent the algorithm conclusions from being improperly endowed with transcendent probative force.

Keywords: artificial intelligence, algorithmic black box, criminal evidence

1. Introduction

Since the industrial revolution in the 18th century, machines have gradually replaced human beings in standardized production and driven changes in all areas of society. 21st century breakthroughs in artificial intelligence have given machines the ability to think in complex ways, such as the DENDRAL chemical analysis system, the MYCIN medical diagnosis system, the AlphaGo Go program, and the ChatGPT dialogue system. The breakthrough development of AI in the 21st century has enabled machines with complex thinking ability, such as DENDRAL chemical analysis system, MYCIN medical diagnostic system, AlphaGo program, and ChatGPT dialog system, etc., which can reach or surpass the level of human beings in professional fields. The resulting "machine evidence" is defined by Andrea Roth as machine-generated data and information. The evolution of machine evidence has gone through three generations: the first generation of semi-mechanized evidence requires human-computer collaboration to complete (such as early mechanical records); the second generation of programmed evidence to achieve fully automated generation (such as electronic data generated by standard processes); and the third generation of Generative Artificial

Intelligence (GAI) evidence[1] is generated by AI with in-depth learning capabilities to generate brand new content on their own, such as medical diagnostic reports, self-driving data, and smart interactive content, etc. The uniqueness of GAI evidence is that it generates innovative content based on self-supervised learning from multimodal big data, rather than simply executing a predefined program.[2] The rapid development of generative AI (AIGC) is reshaping the paradigm of criminal proof, and its technological features provide new tools for judicial efficiency as well as complex challenges of legal application and ethical review.

The introduction of all new types of technology in the criminal sphere is expected to be widely controversial, and so is generative AI evidence. There are views that AI can significantly improve the efficiency and accuracy of criminal proof, and advocate releasing the potential of the technology through legal adaptation.[3] Other scholars have pointed out that the U.S. federal courts have adopted a strict scrutinizing stance on AI evidence, requiring that algorithmic principles and training datasets must be disclosed. For example, in the criminal judgment involving face recognition, the court has repeatedly excluded relevant evidence due to the algorithm's "racial bias" problem, and this kind of technological skepticism is of reference significance to China's judicial practice.[4] As around 2020, the emergence of intelligent sentencing assistance systems under the wave of "intelligent justice" triggered widespread controversy. Now, the emergence of generative artificial intelligence evidence has brought a new round of "technological impact", is bound to trigger a fierce collision of different views. Admittedly, in the face of this unknown but closely related to the interests of the new things, to maintain a reverent and cautious attitude is not wrong. However, in the context of the reality of the increasingly tense judicial resources, academics and practitioners are equally eager to generate artificial intelligence evidence as a powerful tool of proof into judicial practice. Therefore, it has become imperative to clarify the key dilemmas of generative AI evidence in the field of criminal proof, deeply analyze its causes, explore feasible solution paths, and give full play to the positive role of generative AI evidence in criminal proof.

2. The Esoteric Characteristics of Algorithms

On the one hand, the criminal proof of generative artificial intelligence evidence appeared its rising demand, on the other hand, the existing generative artificial intelligence evidence exists into the criminal proof system there are many obstacles, this structural contradiction between supply and demand needs to be solved. To resolve this contradiction and break through the barriers to the application of generative artificial intelligence evidence, the key lies in the essence, clear such evidence is difficult to effectively integrate into the criminal proof system is the root cause of the existing rules of evidence review is difficult to respond to the non-interpretable characteristics of generative artificial intelligence evidence.

First of all, generative AI evidence exists a proof potential that cannot be underestimated. Human society is moving into the age of intelligence, and there are more and more scenarios in which AI can be used. As people become more willing to interact with technology and AI-powered devices, the opportunities for machines to monitor human behavior have greatly increased. The resulting machine evidence may strongly contribute to fact-finding[5]. Relying on technological breakthroughs such as face recognition technology, algorithmic recommendation technology, and intelligent trajectory analysis technology, generative artificial intelligence has entered the evidence law field of vision. At the same time, generative artificial intelligence has further demonstrated its unique potential for discovering the truth of the case on the basis of reflecting its possibility of becoming criminal evidence. Specifically, due to the generative artificial intelligence evidence

[1] The review of GAI evidence discussed in the article includes only the review of judgmental material generated by face recognition, autopilot data, etc., and excludes the review of electronic data material such as videos, recordings, etc., that have been falsified through generative AI techniques.

[2] See Xiong Xiaobiao. (2025). The Dilemma of Generative Artificial Intelligence Evidence Determination and the Normative Approach. *Legal Science (Journal of Northwestern University of Political Science and Law)*, *1*(1), pp. 72-93.

[3] See Gao Manjie & Qin Pengbo. (2024). Criminal Legal Risks and Countermeasures of Generative Artificial Intelligence. *China Judgement*, (13), p. 78.

[4] See Ben Li. (2018). Artificial Intelligence in U.S. Judicial Practice: Issues and Challenges. *China Law Review, 2*(2), pp. 54-56.

[5] Sabina Grace. (2022). Artificial Intelligence in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials. Translated by Fan Wen, *Studies in Procedural Law, 26*, p. 145.

based on massive data, and relatively has the characteristics of good accuracy and high flexibility, so it can be expected to play a unique role in the criminal proof of proof. At the same time, the discovery of the truth of the case is the basic value orientation and one of the ultimate goals of criminal procedure activities[1], and the selection of evidence should also follow this principle. At the same time, according to Article 50 of China's Criminal Procedure Law, materials that can be used to prove the facts of the case are evidence. Therefore, no matter from the perspective of potential proof value of generative AI evidence, or from the perspective of the spirit of the evidence law to encourage the adoption of evidence, the material based on generative AI should be included in the category of criminal evidence.

Secondly, although generative artificial intelligence evidence faces many obstacles in the process of entering the field of criminal procedure, its most fundamental contradiction lies in the fact that the current evidence review system is unable to comfortably cope with the inherent tension between the certainty of machine-generated conclusions and the black box of algorithms. Currently, the academic community believes that the obstacles to the application of generative AI evidence can be categorized as follows: first, the concept is unclear. For the criminal justice application of big data-related evidence, the academic community has initially formed three sets of discourse systems of "big data evidence", "artificial intelligence evidence" and "algorithmic evidence", which to a certain extent has hindered the development of relevant theories. To a certain extent, this has hindered the development of related theories[2]. Secondly, it cannot be accommodated by the legal types of evidence. Third, the risk of human rights infringement, i.e., the source data collection process of generative AI evidence may infringe on the public's right to privacy and other rights and interests. Fourth, the reliability question, i.e., whether the conclusions drawn from generative AI evidence can achieve the state of infallibility presented on its surface.

However, while the above questions better summarize the barriers to criminal proof of generative AI evidence, they collectively ignore the core reason behind the problem, namely the non-interpretability of AI, or the "algorithmic black box", which tends to blur the focus of the issue. First, different terminologies do not present insurmountable barriers, and effective dialog between discourses is often possible. Generative artificial intelligence evidence on criminal proof of the obstacle is essentially human distrust of the conclusions of the machine, so whether it is called big data evidence, artificial intelligence evidence, or algorithmic evidence, scholars are concerned about the content of the focus is the same, and will not create a fundamental obstacle to the relevant discussion. Second, the inability to be accommodated by statutory types of evidence is a constant and common pain point in the history of evidence law. On the one hand, the problem is not relevant to the entry of generative AI evidence into criminal procedure, such as accident investigation reports and other materials actively used in practice to prove the facts of the case are likewise not part of the statutory types of evidence; on the other hand, the problem is based on a specific historical background and legislative reasons, and is not a theoretical discussion of the problem can be resolved. Third, the risk of human rights violations is a problem that exists in all evidence collection, and its core lies in the regulation of the means of evidence collection (such as the additional restrictions of the Criminal Procedure Law on the "technical investigation means"), rather than the main problem of generative AI evidence. Finally, the discussion of the reliability of machine conclusions seems to hit the nail on the head, but the essence of the problem diluted the focus of the problem, for two reasons: First, the reliability of generative artificial intelligence evidence is not necessarily inferior to traditional evidence. For example, in the field of face recognition, the accuracy of artificial intelligence has exceeded that of humans. In the segment of identifying criminal suspects, AI may do better. Second, our system of evidence and proof does not require that evidence in criminal procedure is always 100% reliable, which is also unrealistic. Criminal justice has never pinned its hopes on a certain type of evidential material with transcendent probative power falling from the sky and discovering the truth and proving the

[1] Xiaona Wei. (2024). In Defense of Objective Truth. *The Jurist*, (2), p. 144.

[2] Zhang Di. (2023). Algorithmic Evidence in Criminal Proceedings: Concepts, Mechanisms and Their Utilization. *Journal of Henan University (Social Science Edition)*, (3), p. 36.

facts of a case once and for all. In fact, the criminal proof system formally fully recognizes and accepts the limited nature of individual evidence, thus deriving a set of rules of proof to make use of existing evidence in a more scientific way. This is also true for generative AI evidence. Further, all evidence has the potential to be falsified, and this is where the scientific nature of evidence comes in. In practice, for example, the testimony of witnesses, especially those with an interest in the case, and the confessions and defenses of the accused are not always reliable. Even the once blindly superstitious "appraisal opinion" is sometimes wrong. In view of this, the lack of reliability is not a fundamental obstacle to the entry of artificial intelligence into criminal proof.

Looking beyond the appearance of "unreliability" of generative AI evidence and tracing the underlying causes of this impression, it can be found that the fear of generative AI evidence stems more from its inherent mystery, i.e., its non-explainability. Because of this unknown, the criminal proof system can not give its own value equivalent to the effectiveness of the proof, and therefore unlimited worry about whether such evidence to give too much trust. However, from the perspective of the overall development trend of artificial intelligence, the massive corpus, multimodal features and autonomous production of artificial intelligence will continue to deepen, and the technical interpretability will be further weakened. Non-interpretability is essentially a natural attribute of AI products, and interpretability can only be used as a governance orientation. The White Paper on Artificial Intelligence Safety Standardization released in 2023 states that "algorithmic models are becoming increasingly complex, and the goal of interpretability is difficult to achieve", and it is becoming extremely difficult for human beings to understand the large-model AI, and it is currently being explored in the direction of explaining large models with the help of AI. It can be seen that the non-interpretable nature of generative AI is outstanding, but as a "techno-social" paradigm, the social side of the society cannot put itself "on the shelf".[1]

3. Deconstructing the Black Box: Algorithmic Bias in Criminal Justice Systems

Algorithmic black box refers to the non-disclosure and non-transparency of AI algorithms,[2] the non-explainable characteristic may either originate from the algorithmic secrecy behavior for commercial purposes, i.e., the subject concerned does not want the law of the algorithm's operation to be disclosed; or it may also originate from the nature of the algorithm itself, i.e., the algorithmic part is impossible to be interpreted. Specifically, in the field of machine learning, there is a trade-off between model interpretability and model performance (accuracy). Several models (including linear regression and decision trees) have predictive principles that are well understood intuitively, but require a sacrifice in model performance because they produce results with high bias or variance (underfitting: linear models), or are prone to overfitting (tree-based models). More complex models such as integrated models and the recent rapid development of deep learning often produce better predictive performance, but are considered black-box models because it is extremely difficult to explain how these models actually make decisions. The lack of clarity in the decision-making process makes AI face three major interlocking and stepwise obstacles, namely the lack of argumentation, the problem of qualification and the crisis of trust.

Non-interpretability itself does not point to damage, but the risks arising from non-interpretability are directly damaging. Combined with the occurrence of risk, the risk mainly appears in the security of the system itself, the value of the user, and the basic rules of social operation.[3]

3.1 The Absence of Argumentation: Institutional Alienation in the Criminal Proof Process

Criminal proof is a bridge between the evidentiary material and the truth of the case and is processual. In fact, the process of legal argumentation reflects the value of procedural justice.[4] However, the inherent algorithmic black-box characteristics of artificial intelligence

[1] Longjun Jin. (2025). The Uninterpretability of Generative AI and Its Rule of Law Response. *Rule of Law Research*, (2), p. 43.

[2] Feng Xu. (2019). Legal Regulation of the Algorithmic Black Box of Artificial Intelligence — Expanding on the Example of Intelligent Investment Guarantees. *Oriental Law, 6*(6), pp. 78-86.

[3] Longjun Jin. (2025). The Uninterpretability of Generative AI and Its Rule of Law Response. *Rule of Law Research*, (2), p. 47.

[4] See Wei Bin. (2024). Analysis of Legal Arguments for the Explanatory Difficulties of Judicial Artificial Intelligence. *Legal System and Social Development*, (4), pp. 76-92.

technology lead to the generation of artificial intelligence evidence that often manifests itself as "assertive" conclusions, which conflicts with the processual attributes of criminal proof and fails to satisfy the requirements of justice for procedural transparency, which may jeopardize procedural justice.

Specifically, the essence of criminal proof is the process of reconstructing factual knowledge through evidence retrospection. All evidentiary materials used for conviction and sentencing should satisfy the basic attribute of objectivity, and should be presented in the trial in a form that is original, direct and directly reflects the facts of the case, refusing to use processed, value-biased conclusive materials as evidence in the case. This is the best evidence rule and opinion evidence rule jointly constructed evidence jurisprudence foundation. Based on this, the adjudicator through their own professional knowledge and rational judgment to build a bridge from the evidence material to the facts of the case, and ultimately through the argument and evidence of reasoning in the process of determining the evidence and reasoning to fully explain, so that it is figurative and public, which is the fact that the reasoning and the application of reasoning of the law and the premise and foundation of the reasoning of the[1], but also criminal proof of the meaning of the due. However, generative artificial intelligence evidence is the conclusion of the machine deduction, and the general evidence material presents the basic, objective facts of the case is different, its nature and "appraisal opinion" similar, but can not and appraisal opinion of the same trace the conclusion of the deduction of the trajectory and reasoning process. The existence of algorithmic black box leads to the machine can output conclusions, but can not clarify its reasoning process. This flaw makes it difficult for the adjudicator to theoretically rule out other possibilities and substantively meet the standard of proof beyond a reasonable doubt. This inherent logical rupture, so that the generation of artificial intelligence evidence as if "foreign objects", alienated into the public prosecutor's office to pursue the conviction of instrumentalized means. At the same time, due to the generative artificial intelligence evidence of non-interpretability, so that the evidence review is alienated into a simple verification of the results. As shown in the U.S. case of Wisconsin v. Loomis (State v. Loomis), when the algorithmic logic of the COMPAS recidivism risk assessment system could not be disclosed, the judge was forced to shift the focus of the review from the reasoning process to the conclusion probability.[2]

Further, this conflict will lead to a cognitive break in the rationality of judicial decision-making. Procedural justice requires that the adjudicator must show the formation process of evidence through the "adjudication documents fully reasoned". However, the non-interpretability of algorithms leads to a cognitive break between "technical rationality" and "judicial rationality". "When technical decision-making cannot be translated into a human-understandable logic chain, the judge's discretion will be reduced to an endorsement tool for the algorithm's output." This unknowability of the decision-making process essentially violates the "duty to justify" required by procedural justice.

3.2 The Challenge of Cross-Examination: The Loss of the Voice of the Defense

Currently, the common law system and civil law system countries have formed a consensus: the right to confrontation is a fundamental right of the citizens, the right to confrontation is the basic obligation of the state to the citizens,[3] the legitimacy of the basis behind it, including, but not limited to, the right of defense, the authenticity of the government to prevent the abuse of power, and to promote the trust of the state power and a variety of other theories[4]. Article 61 of China's Criminal Procedure Law stipulates that "witness testimony must be examined in court by the public prosecutor, the victim and the defendant, the defense, and both sides and verified before it can be used as the basis for a decision", which likewise clarifies the

[1] Wang Zeshan. (2024). Study on the Reasoning of Evidence Authentication in Criminal Judicial Documents. *Journal of China University of Political Science and Law*, (1), pp. 238-252.

[2] Cited in Jiang Su. (2020). Automated Decision-making, Criminal Justice and the Rule of Law on Arithmetic — Reflections Triggered by the Loomis Case. *Oriental Law Journal*, *3*(3), pp. 76-88.

[3] Fan Chongyi & Wang Guozhong. (2006). A Brief Exploration of the Right of Criminal Defendants to Confront Evidence. *Journal of Henan Province Cadre College of Politics and Law Management*, (5), pp. 49-57.

[4] See Chen Yongsheng. (2005). On the Defense's Right to Examine Evidence in Court. *Law and Business Studies*, (5), pp. 89-96.

defense's right to examination. At the same time, the defendant's right to speak in criminal procedure in China is often crystallized in his right to give evidence in court, and the degree of its realization is closely related to whether it is possible to realize the dual values of discovering the truth of the case and safeguarding human rights. Further, with the de-instrumentalization of the value of criminal procedure, the right to confrontation has evolved in contemporary times into a symbol of procedural justice.

The criminal defendant's right to confrontation is the defendant's right to refute and question the prosecution's evidence in court[1], which can be divided into the right to confrontation and the right to cross-examination. Whether it is the right of confrontation, or the right of cross-examination implies a basic premise: that is, a comprehensive understanding of the prosecution's evidence, that is, the defense has a clear understanding of the prosecution's allegations, the evidence used to prove its allegations and its chain of logical proof. Therefore, most countries have set up a relevant system regarding the discovery of evidence. In the context of generative artificial intelligence evidence, when the algorithmic decision-making process becomes a "technological black box", the defense will encounter structural barriers to the right of defense, the defense often does not have access to all the information about the evidence, and the logical chain from the source of data to the conclusion of the evidence to the facts to be proved is broken. According to Article 13 of the European Parliament's Artificial Intelligence Act, algorithmic interpretability constitutes a prerequisite for the exercise of a party's right to object. Algorithm non-interpretability directly leads to the defense can not be generated for the logic of evidence to put forward effective questioning, in essence, hollowed out the defense to the party's "evidence, questioning, debating" rights bundle, which puts it into a "no evidence can be qualitative" predicament, which directly affects its in the court hearing process. The realization of the right to speak, contrary to the requirements of the principle of "equality of arms", leading to the degradation of the litigation structure from a "confrontation between two creations" to a "monopoly of technical authority".

[1] Wang Xiaohua. (2012). Research on the Right of Criminal Defendants to Confront Evidence in China. Southwest University of Political Science and Law.

3.3 Crisis of Confidence: Lack of Credible Outcomes

Generative AI evidence at the level of argumentation of the logical ring break and the resulting restrictions on the right of the defense to confrontation, directly leading to a crisis of credibility corresponding to the outcome of the referee. Judicial credibility refers to the general knowledge and degree of trust held by the public in the impartiality and authority of the judicial system, the essence of which is the social credibility accumulated by the judicial organs through the fulfillment of their duties by adhering to the legal norms and respecting the objective facts. This concept not only reflects the people's expectations for fairness and justice in justice, but also reveals the core objectives and operating rules of the judicial system, and is a key indicator for assessing the degree of development of the rule of law civilization in a country or region.[2]

The people's trust in the adjudication of a case mainly comes from two dimensions: substantively, whether the adjudication result is correct, i.e., whether the link between the facts of the case and the adjudication result is logical; and procedurally, whether the process of arriving at the adjudication result is flawless, i.e., whether every subject with an interest in the case equally and voluntarily expresses his or her own opinion. When machine conclusions drawn by AI are used as evidence for conviction and sentencing, these two drawbacks are simultaneously revealed by the existence of the algorithmic black box. On the one hand, the lack of argumentation leads to the substantive defects of the adjudication results; on the other hand, the impairment of the defense's right to cross-examination directly weakens the procedural legitimacy of the adjudication results. There is no reason for the public not to fear and question a conclusion that is both procedurally and substantively flawed, while at the same time disposing of the fundamental rights of the accused.

The credibility of judicial decisions is built on the dual basis of substantive legitimacy and procedural legitimacy. At the substantive level, the conclusion of the decision must form a close logical loop with the facts of the case as proven by the evidence; at the procedural level, it is

[2] See Long Zongzhi. (2015). Realistic Factors Affecting Judicial Justice and Judicial Credibility and Their Countermeasures. *Contemporary Jurisprudence*, (3), pp. 3-15.

required that the decision-making process safeguard the right of all parties to participate in the litigation, and that "visible justice" be constructed through equal dialog. This dual legitimacy constitutes the core value of the modern judicial system. However, when the conclusion of the machine generated by artificial intelligence is directly used as the basis for conviction and sentencing, the algorithmic black box will simultaneously dismantle the legitimacy of these two dimensions of the foundation. First, in the entity level, the non-traceable algorithmic reasoning makes the factual determination reduced to "technical arbitration", the correlation between the adjudication results and the facts of the case lost verifiable basis, resulting in the substance of the justice of the entity is reduced to a probabilistic judgment; Secondly, in the procedural level, the non-explanatory algorithmic decision-making essentially deprives the defense of the right to effective questioning, and the foundation of procedural justice has been hollowed out. The foundation of justice has been hollowed out. The loss of this dual legitimacy will lead to a serious crisis in the rule of law: a decision that is neither substantively correct nor procedurally participatory is able to dispose of the fundamental rights of citizens. This potential risk of "algorithmic tyranny" will not only trigger public skepticism about the adjudication of individual cases, but will also fundamentally shake the trust in the judicial system. "Justice must not only be realized, but also realized in a visible way."[1] Otherwise, the foundation of the rule of law edifice will be in danger of collapsing.

4. Deconstructing and Overcoming Algorithmic Black Boxes in Evidentiary Procedures

As mentioned earlier, the fundamental obstacle to generative AI evidence in criminal proof activities does not lie in its lack of reliability, but in the subjects of its non-interpretability of the "fear", the seemingly "unquestionable" face of science and its internal operating logic. There is a strong tension between the seemingly "unquestionable" face of science and the mysterious color of its inner logic of operation. In essence, the value of technical agnosticism and judicial refutable conflict. The process of criminal proof requires that the evidence must be interpretable, questionable, can be overturned open characteristics, and algorithmic black box created by the "technological leviathan" is eroding the procedural justice depends on the existence of the system foundation. In view of this, this structural contradiction determines the key to the problem is to re-examine the ability of generative artificial intelligence evidence boundaries, the establishment of a targeted review system, so that the subjects get to know, question, overthrow the conclusions of the machine's right and ability, rather than to ensure that the generative artificial intelligence evidence of the "one hundred percent" accuracy, this is the problem of the technical field, rather than the black box of algorithms created "technological leviathan" is eroding the system on which procedural justice is based. This is a technical issue, not a judicial one. To break the myth of certainty of generative artificial intelligence evidence in the field of criminal proof, we can establish a corresponding challenge system from the content and method of review. Generative artificial intelligence evidence that has been effectively challenged and incorporated into the basis for a final decision meets the requirements of procedural justice and can also respond to the public's expectations for justice.

4.1 Systematic Review: Transparency in the Mechanism of Evidence Generation

It is true that, theoretically, there is an inherent "cognitive blind spot" in the process of generating artificial intelligence evidence, and this technical limitation should not be a reason for abandoning regulation. On the contrary, we should uphold the principle of "limited transparency", within the boundaries of technical possibilities to actively promote the transparency of the relevant content, the part that can be reviewed to establish a perfect system. First of all, the most front-end and fundamental issue is the raw data on which the machine's conclusions are based. It needs to face at least twofold challenges of authenticity and comprehensiveness. Both the quantity and quality of data are directly related to the accuracy of the final conclusion. Secondly, on the middle end, the main focus is on the review of algorithms. Although the research on algorithmic review is not fully developed at present, there is a more mature consensus on the way to review scientific evidence of the same

[1] Alfred Thompson. (2011). *Denning: Due Process of Law*. Translated by Li Keqiang and others, Law Press.

nature: in 1923, the U.S. Court of Appeals for the District of Columbia federal appeals court in the case of Frye v. United Stated laid down a standard for measuring the reliability of expert testimony, which held that the court accepts a recognized scientific theory. In Frye v. United Stated, the U.S. Court of Appeals for the District of Columbia set forth the standard for measuring the reliability of expert testimony, holding that a court will accept expert testimony derived from an accepted scientific theory or scientific discovery, provided that what is deductively inferred therefrom is sufficiently well grounded and generally recognized in the field of which it is a part[1], i.e., the "Frye standard". Finally, at the end, there should be a qualification process for those who operate AI systems. Reference can be made to the rules for qualifying personnel in the appraisal review system.

4.2 Equally Armed: Expert Auxiliary Assistance

Aiming at the artificial intelligence into the criminal procedure, the resulting impact of the prosecution and defense power contrast, scholars put forward the concept of "evidence bias"[2] to argue that the right to confrontation has been eroded to a certain extent due to the introduction of generative artificial intelligence evidence. Undoubtedly, to give the weaker side of the stronger force clamping is the most direct means of solving the problem of "bias in".

In the application scenario of generative AI evidence, the imbalance in the ability of the defense party is centered on the structural weakness of the technical nature of the evidence power. Due to the high degree of asymmetry in algorithmic information, although the defense is generally involved in the AI service ecosystem, it faces the following dilemmas: first, it lacks accessibility to the underlying algorithmic architecture and model training logic of generative evidence; and second, it has a blind spot to the technical paths by which personal data are extracted, labeled, and embedded in decision-making systems. Even if the parties are able to recognize the importance of collecting generative AI evidence, they are often caught in a double passivity due to the black box effect of algorithms and the lack of professional dialogue capabilities: it is difficult to analyze the logic and causal chain of generating AI evidence, and they are also unable to effectively challenge the semantic completeness of its output, which ultimately results in the alienation of technological empowerment into the ability to fight against the litigation bias. Based on this, the permission to seek professional help and as an effective basis for questioning the generation of artificial intelligence evidence is the context of the prosecution and defense of the two sides of the basic requirements of equal arms. In view of the commonality between generative AI evidence and appraisal opinions in many aspects[3], reference can be made to the setting of expert assistants in the current appraisal opinion system in China.

Specifically, through a reasonable definition of the qualifications of the expert supporter, improve the rights and obligations of the expert supporter to participate in the litigation, and clarify the litigation status of the expert supporter and the attributes of his opinions, etc., to ensure that the role of the expert supporter can be given full play to, and to ensure that the rights and interests of the person being prosecuted can be effectively safeguarded. At the same time, the content of the expert auxiliary's examination of the generative artificial intelligence evidence can refer to the interpretation made by the U.S. Federal Supreme Court in 1995 in the case of Daubert v. Merrell Dow Pharmaceuticals. Inc. on the issue of scientific standard of scientific evidence. The decision held that the reliability of expert testimony should be judged from four aspects: (1) whether the scientific theory and scientific methodology relied upon to form the expert testimony can be repeatedly tested; (2) whether the scientific theory and scientific methodology used to form the expert testimony has been peer-reviewed or has been published; (3) whether the known or potential rate of error concerning the theory is acceptable; (4) whether the theory and research methodology guiding the theory in question are relevant to the case; and (5) whether the scientific standard for scientific evidence is acceptable. Methodology and research methods are accepted by the

[1] See Frye v. United States, 293 F. 1013, 1014 (D.C. Cir. 1923).

[2] See Zhang Qi and Fan Yunhui. (2024). The Risks of Artificial Intelligence Evidence in Judicial Activities and Legal Responses. *Journal of Henan Finance and Economics College (Philosophy and Social Science Edition)*, (1), pp. 35-40.

[3] See Zheng Fei, Ma Guoyang. (2022). The Triple Dilemma and the Way Out of the Application of Big Data Evidence. *Journal of Chongqing University (Social Science Edition)*, (3), pp. 207-218.

relevant scientific community and the extent of that acceptance[1].

4.3 Practical Verification: Historical Data Disclosure

The transparency of the evidence generation mechanism and the support of expert assistants to the defense try to guarantee the possibility of challenging the evidence of generative AI at the institutional level, and to convey to the public the notion that the adjudication results are logically correct. However, it cannot be ignored that due to the non-interpretability of artificial intelligence, there will always be a part of the path of machine conclusion proof that is in the gray area. Therefore, in line with the spirit of the evidence law, "strengthen the evidence rule", the proof of the existence of flawed evidence should be strengthened. Given that the underlying logic of generative artificial intelligence evidence comes from the science of machine learning, the historical accuracy of the algorithms on which it is based can be publicized for practical verification, thereby enhancing the credibility of the results.

Historical data disclosure has a number of advantages. First, the approach helps the general public make clear judgments. "Mathematical certainty is absolute." Accuracy as a number can turn ambiguity into clarity and help the public make judgments. Second, the approach is easy to understand. Size judgments are simpler. The disclosure of historical data is more publicized than the disclosure of algorithms, and has a more significant effect on improving the credibility of adjudication results.

5. Conclusion

In his book *Technopoly*, communication scholar Neil Bozeman asserts that every new technology is both a burden and a gift, not an either/or outcome, but a product of both advantages and disadvantages. Generative AI evidence may be a technological breakthrough or a Pandora's box that has already been opened in criminal proof activities. To some extent, the fear of the latter stems from the opacity of the algorithm. Humans are naturally afraid of the unknown, for humans, the algorithm operates like a "black box" — we are responsible for providing data, models and architecture, the algorithm is responsible for giving the answer, while the middle of the operation process is only carried out in the dark. This kind of cooperation seems to bring us great convenience, but the problem is that if the operation of the algorithm is not monitorable and unexplainable, it will lead to the fact that human beings can't really understand the algorithm, and they can't control the algorithm effectively, and thus can't foresee and solve the problems that the algorithm may bring[2].

In light of this, the obstacles to generative AI evidence in criminal proof should be clarified by focusing on its non-interpretability. Further, criminal justice does not need to be committed to the technological breakthroughs therein, but should focus on the subtle tension between the certainty of the machine's conclusions and its mysteriousness, so that generative AI evidence will always have the possibility of being challenged, and as far as possible to ensure that it will not be given a probative value that far exceeds its own proper value. This is the necessary path for generative AI evidence to gain trust and ultimately smooth criminal procedure.

References

Alfred Thompson. (2011). *Denning: Due Process of Law*. Translated by Li Keqiang and others, Law Press.

Ben Li. (2018). Artificial Intelligence in U.S. Judicial Practice: Issues and Challenges. *China Law Review, 2*(2), pp. 54-56.

Chen Yongsheng. (2005). On the Defense's Right to Examine Evidence in Court. *Law and Business Studies*, (5), pp. 89-96.

Fan Chongyi & Wang Guozhong. (2006). A Brief Exploration of the Right of Criminal Defendants to Confront Evidence. *Journal of Henan Province Cadre College of Politics and Law Management*, (5), pp. 49-57.

Feng Xu. (2019). Legal Regulation of the Algorithmic Black Box of Artificial Intelligence — Expanding on the Example of Intelligent Investment Guarantees. *Oriental Law, 6*(6), pp. 78-86.

Gao Manjie & Qin Pengbo. (2024). Criminal Legal Risks and Countermeasures of Generative Artificial Intelligence. *China Judgement*, (13), p. 78.

[1] See Daubert v. Merrell Dow Pharms., 509 U.S. 579, 594 (1993).

[2] Wang Huanchao. (June 13, 2019). How to Make Algorithms Explain Why They "Algorithmically Discriminate"?. Tencent Research Institute.

Jiang Su. (2020). Automated Decision-making, Criminal Justice and the Rule of Law on Arithmetic — Reflections Triggered by the Loomis Case. *Oriental Law Journal*, *3*(3), pp. 76-88.

Long Zongzhi. (2015). Realistic Factors Affecting Judicial Justice and Judicial Credibility and Their Countermeasures. *Contemporary Jurisprudence*, (3), pp. 3-15.

Longjun Jin. (2025). The Uninterpretability of Generative AI and Its Rule of Law Response. *Rule of Law Research*, (2), p. 43, 47.

Sabina Grace. (2022). Artificial Intelligence in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials. Translated by Fan Wen, *Studies in Procedural Law, 26*, p. 145.

Wang Huanchao. (June 13, 2019). How to Make Algorithms Explain Why They "Algorithmically Discriminate"?. Tencent Research Institute.

Wang Xiaohua. (2012). Research on the Right of Criminal Defendants to Confront Evidence in China. Southwest University of Political Science and Law.

Wang Zeshan. (2024). Study on the Reasoning of Evidence Authentication in Criminal Judicial Documents. *Journal of China University of Political Science and Law*, (1), pp. 238-252.

Wei Bin. (2024). Analysis of Legal Arguments for the Explanatory Difficulties of Judicial Artificial Intelligence. *Legal System and Social Development*, (4), pp. 76-92.

Xiaona Wei. (2024). In Defense of Objective Truth. *The Jurist*, (2), p. 144.

Xiong Xiaobiao. (2025). The Dilemma of Generative Artificial Intelligence Evidence Determination and the Normative Approach. *Legal Science (Journal of Northwestern University of Political Science and Law)*, *1*(1), pp. 72-93.

Zhang Di. (2023). Algorithmic Evidence in Criminal Proceedings: Concepts, Mechanisms and Their Utilization. *Journal of Henan University (Social Science Edition)*, (3), p. 36.

Zhang Qi and Fan Yunhui. (2024). The Risks of Artificial Intelligence Evidence in Judicial Activities and Legal Responses. *Journal of Henan Finance and Economics College (Philosophy and Social Science Edition)*, (1), pp. 35-40.

Zheng Fei, Ma Guoyang. (2022). The Triple Dilemma and the Way Out of the Application of Big Data Evidence. *Journal of Chongqing University (Social Science Edition)*, (3), pp. 207-218.

PIONEER
ACADEMIC PUBLISHING LIMITED

Studies in Law and Justice
ISSN 2958-0382
www.pioneerpublisher.com/slj
Volume 4 Number 3 June 2025

An Appraisal of the Role Played by State Courts in Combating Medical Negligence in Cameroon: A Review of Selected Case Laws

Agbor James Eyong[1]

[1] Ph.D., University of Buea, Cameroon
Correspondence: Agbor James Eyong, Ph.D., University of Buea, Cameroon.

doi:10.56397/SLJ.2025.06.02

Abstract

This paper critically appraises the role of state courts in combating medical negligence in Cameroon through a review of selected judicial decisions. The research adopts a qualitative methodology, relying on doctrinal analysis and case study approaches to explore the effectiveness, consistency and limitations of judicial responses to medical negligence and malpractices. By examining a purposively selected sample of landmark cases from Cameroonian courts, the study assesses how legal principles are interpreted and applied, the adequacy of judicial remedies and the broader implications for patients' rights and healthcare accountability. The findings reveal a gradual, yet uneven evolution in judicial attitudes towards medical negligence, marked by procedural delays, limited expertise in medical matters and inadequate enforcement of judgments. The paper concludes that while courts have an essential role in promoting accountability and deterrence, there is a pressing need for judicial reforms, capacity building and enhanced legal frameworks to ensure justice for victims of medical negligence in Cameroon.

Keywords: role played, state courts, combating, medical negligence, Cameroon, review of selected case laws

1. Introduction

The practice of medicine has existed from time immemorial which is why medical practice is often regarded as a profession of great antiquity.[1] The medical profession or medical practice evolved to maintain and restore human health by the prevention and treatment of illnesses in human beings. By exercising their profession or sworn duty, medical practitioners have inadvertently been engaged in the protection of human rights over the years. Negligence within the context of the medical profession has become the order of the day in modern societies. In fact, it is an established rule of law that physicians/medical personnel owe their patients a duty of care. In the 1800s, Oliver Wendell Holmes Jr., an American Judge, carried out a study wherein he examined the history of negligence, in search of a general theory of tort. He concluded that from earliest times in

[1] Ezinne Vivian & Chidinma Blessing Nwakoby, 'Medical Negligence in Nigeria.' *Journal of Education, Humanities, Management & Social Sciences (JEHMSS),* (2013) pp. 7-28.

England, the basis of tort liability was fault or failure to exercise due care.[1]

The existence of this duty is predicated on the right to life, which is a sacrosanct right under international law. In a bid to protect the right to life and the right to the highest attainable standard of health, physicians have a duty to take care *vis-à-vis* their patients. The duty of care in this connection falls within the context of medical negligence, and over the years, medical negligence has often arisen where the degree of care required is not observed. [2] Medical negligence and malpractices have become a growing concern in the world today, characterized by the difficulty, and in some countries, the inability of victims to go about seeking justice and redress. Even though English common law has for a long time imposed a liability for the unjust acts of others,[3] it was only during the earlier part of the 19th century when the industrial revolution was induced by a series of accidents caused by industrial machinery that negligence started to gain acknowledgement as a distinct and independent base of tortious liability.[4]

The idea of the duty of care has over the years been considered to be founded on the assumption that in a civilized and developed society, every person has an obligation not to cause injury to his neighbour, and that there should be liabilities for failure to exercise due diligence in the exercise of one's profession.[5] Within the context of the law of torts,[6] the duty of care is a legal obligation levied on an individual, requiring adherence to a standard of reasonable care while performing any act that will possibly or foreseeably cause harm to another.[7]

Over the years in the medical field, the responsibility of a medical personnel is to offer professional care to sick persons who do not have the ability to help themselves. It follows that from time immemorial, a legal duty has always been imposed on physicians to exercise professionalism in terms of the provision of the highest attainable standard of care to people placed under their watch (patients). As far back as 1937, it had already been recognized that there was a dwindling old-time relationship of mutual confidence between doctor and patient upon which the practice of medicine depended.[8] More so, studies and research have over the years revealed evidence of medical negligence, manifested in the form of: staff's rudeness, lack of care and concern for patients, failure to administer the right medication, mistakes in diagnoses, negative attitudes to patients, leaving or forgetting surgical instruments in the bodies of patients, etc.[9] In a bid to ensure strict application of the duty of care in the medical profession, mechanisms have over the years been laid down. In Cameroon for example, for a person to practice medicine, he must be professionally qualified and fulfil the conditions set out in the laws regulating the practice of medicine.[10]

It is worth noting that the ancient concept of the duty of care was first articulated by Brett M.R in 1883 in the case of *Haven v. Pender.*[11] In this case, Brett M.R clearly stated that:

"Wherever one person is… placed in such a position with regard to another that everyone of ordinary sense… would at once recognise that if he did not use ordinary care and skill… he would cause danger or injury to the person or the property of the other, a duty arises to use ordinary care and skill to avoid such danger."[12]

The concept of the duty of care was further developed by Lord Atkin in the landmark case of *Donoghue v. Stevenson.*[13]

---

[1] Oliver Wendell Holmes Jr. (1881). *The Common Law.* London: Macmillan.

[2] Oseni T.I.A. (2019). Medical Duty of Care: A Medico-Legal Analysis of Medical Negligence in Nigeria. *American International Journal of Contemporary Research, 9*(1), pp. 56-63.

[3] Such as medical negligence.

[4] Hassan King Obaro. (n.d.). Legal Imperatives of Medical Negligence and Medical Malpractice. Available online at: https://www.njmonline.org. Accessed on January 28, 2024.

[5] *Ibid.*

[6] A Tort is a civil wrong, breach of which remedy is a civil action for liquated or unliquidated damages.

[7] Chris Turner. (n.d.). *Unlocking Torts,* 4th Edition. London: Routledge Publishing. p. 26.

[8] E. Pierre Gould. (1937). The Defence of Medical Negligence. *Medico-Legal Criminological Review, 5*(2), pp. 191.

[9] Campbell. D. (2011). Hospital Patients Complain of Rude Staff, Lack of Compassion and Long Waits. The Guardian. Available online at: https://www.theguardian.com/society/2011/feb/23/hospital-patients-rude-staff-long-waits. Accessed on January 28, 2024.

[10] Law No. 80/6 of 14 July 1980 to Regulate the Practice of Medicine in Cameroon; Law No. 80/7 of 14th July 1980 to Organize the Medical Association in Cameroon.

[11] (1883) 11 QBD 503.

[12] Brett M.R in *Haven v. Pender* (supra).

[13] (1932) AC 562.

In this 1932 case, Donoghue and her friend stopped for a drink at a café. The friend ordered the drinks and paid for them. Donoghue's drink, ginger beer, was supplied in a dark opaque bottle. She filled her class and drank some of the contents. As she poured the rest of the contents, (the dregs) out of the bottled, a partially decomposed snail fell out of the bottle into the glass. Donoghue became very ill suffering nausea, gastro-enteritis and shock. As it was a friend who bought the drink for her, Donoghue was unable to sue in her own right in contract because of the doctrine of privity of contract. She nevertheless sued and claimed £500 damages from the manufacturer for his negligence and was successful. The House of Lords was prepared to accept that there could be liability on the manufacturer, even though there was lack of a contractual relationship (privity of contract) between the manufacturer and the claimant.

Lord Atkin applied a new rule of law to this case, "the duty of care". As he put it:

"you must take reasonable care to avoid acts or omissions which you can reasonably foresee would be likely to injure your neighbour. Who then in law is my neighbour? …persons who are so closely and directly affected by my acts, that I ought reasonably to have them in my contemplation as being so affected when I am directing my mind to the acts or omissions in question."[1]

Lord Atkin's Neighbour principle provides that as far as there exists foreseeability of harm, then failure to observe reasonable care translates into negligence.

Also, in the words of Alderson. B in the case of *Blyth v. Birmingham Waterworks Co.*[2] "Negligence is the omission to do something which a reasonable man, guided upon those considerations which ordinarily regulate the conduct of human affairs would do, or doing something which a prudent and reasonable man would not do."[3] This definition by Alderson B raises questions as to who is a reasonable man.

Medical negligence is a form of negligence common today as a result of the absence of professionalism in the exercise of the medical profession. Over the years, medical practitioners have been held liable for professional negligence when they fail to exercise their skills or acts with the degree of care expected of their experiences and status in the process of attending to a patient.[4] The issue of medical negligence is founded on the non-provision of the duty of care owed to the patient. Michael A. Jones with regard to the issue of medical negligence stated that:

"Normally, there will be no difficulty in finding a duty of care owed by the doctor to his patient, at least where the claim is in respect of personal injuries, and this is true even when there is a contractual relationship. The practitioner may also owe a duty of care to the patient in respect of pure financial loss. In addition, there are a number of circumstances where a doctor may also owe a duty of care to a third party, arising out of the treatment given to the patient, but the incident and extent of such duties are more problematic."[5]

Also, in the case of *Cassidy v. Ministry of Health*[6] Lord Denning stated that:

"In my opinion, authorities who run a hospital, be they local authorities, government boards, or any other corporation, are in law under the self-same duty as the humblest doctor. Whenever they accept a patient for treatment, they must use reasonable care and skill to cure him of the ailment. The hospital authorities cannot of course do it by themselves. They have no ears to listen through the stethoscope, and no hand to hold the knife. They must do it by the staff and if the staff are negligent in giving treatment, they are just as liable for that negligence as anyone else who employs others to do his duties for him. Is there any possible difference in law, I ask, can there be, between hospital authorities who accept a patient for treatment and a railway or shipping authorities who accept a passenger for carriage? None whatever. Once they undertake the task, they come under a duty to use in doing of it, and that is so whether they do it for reward or not."[7]

The issue of whether or not a medical

[1] *Ibid.*

[2] (1956) 11 EX Ch 781.

[3] *Ibid.*

[4] This may happen when he fails to provide prompt attention and care to a patient requiring emergency care, when he was in a position to do so. When harm results from the delay in attending to a patient (when such delays could have been avoided) then the medical practitioner is liable for medical negligence.

[5] Michael A. Jones. (1996). *Medical Negligence* (London: Sweet & Maxwell), p. 29.

[6] (1951) 2KB 343.

[7] *Ibid.*

practitioner owes a duty of care has over the years been regarded as a matter of law to be determined by the courts. In terms of medical negligence, the term 'duty of care' is synonymous to the concept of an 'undertaking' towards a patient. In the case of *Cassidy v. Ministry of Health*[1], Lord Denning stated that "In my opinion, authorities who run a hospital, be they local authorities, government boards, or any other corporation, are in law under the self-same duty as the humblest doctor. Whenever they accept a patient for treatment, they must use reasonable care and skill to cure him of the ailment…"

The duty of care within this context involves: (a) a duty to possess special skill and knowledge (b) a duty to exercise caution in treatment/diagnosis (c) a duty to exercise due diligence, care, knowledge and skill and (d) a duty to provide prompt responses to emergencies.[2] In other words, the moment a physician assumes responsibility towards a patient, the duty of care is established.

As earlier mentioned, in order to prove medical negligence or medical malpractice, four important elements must be established: firstly, a professional duty must be owed to the patient; second, there must be a breach of such duty; thirdly, injury must have been caused by the breach; and fourthly, the breach of professional duty must result in damages.

In the 2014 South African case of *Lushaba v. MEC for Health, Gauteng*[3] the courts were able to prove all these elements. Similarly, these elements were proven in the Ugandan case of *Kimosho v. Wakapita & 2 Others*[4] where Wakapita unlawfully and negligently prescribed a drug to the plaintiff which eventually put her life and the life of her unborn child at risk. She subsequently suffered a miscarriage. The court in this case found that all the elements for medical negligence had been satisfied and held that Wakapita as a medical personnel acted negligently and that his employer was vicariously liable for his professional negligence. In awarding damages, the court held that Wakapita and his employer were jointly and severally liable for compensation to the plaintiff. The judgment thus held both the medical institution and the medical professional liable jointly and severally for medical negligence. The reasoning of the court in delivering such a judgment was that it will ensure due diligence by medical professionals in carrying out their duties.

2. National Legal Frameworks for the Protection of the Right to Health in Cameroon

Several legal measures have been adopted at the Cameroon national level to protect and promote the right to health. These legal measures are discussed in this subsection.

2.1 Law No. 96/6 of 18th January 1996 as Amended and Supplemented by Law No. 2008/001 of 14 April 2008 on the Cameroon Constitution

The constitution of the Republic of Cameroon is the highest law of the land and makes valuable strides towards the protection of human rights including the right to health. The constitution plays a crucial role in safeguarding the fundamental right to health for its citizens. This right is enshrined in the preamble which is a replica of the Universal Declaration of Human Rights.

Firstly, the preamble of the Cameroon constitution in an attempt to guarantee all fundamental human rights including the right to health of all Cameroonians states that:

"We, the people of Cameroon, Declare that the human person, without distinction as to race, religion, sex or belief, possesses inalienable and sacred rights;

Affirm our attachment to the fundamental freedoms enshrined in the Universal Declaration of Human Rights, the Charter of the United Nations and The African Charter on Human and Peoples' Rights, and all duly ratified international conventions relating thereto..."[5]

A perusal of the aforementioned provision reveals that the constitution strives to protect all fundamental human rights recognized under international law instruments such as the UDHR, the African Charter and other human rights instruments, including the right to health.

Furthermore, the preamble inadvertently

[1] (1951) 2KB 343.

[2] Guptha Jaiprakash. (2002). *Ethics and Law Controlling Medical Practitioners*. Available online at: https://www.aironline.in/legal-articles/Ethics%20and%20Law%20-Controlling%20Medical%20Practitioners. Accessed on January 17th, 2024.

[3] (2014) ZAGPJHC 407.

[4] (2018) UGHCCD 71.

[5] Paragraph 4 & 5 of the Preamble, Law No. 96/6 of 18 January 1996 as amended and supplemented by Law No. 2008/001 of 14 April 2008 on the Cameroon Constitution.

protects the right to health by stating that:

"every person has a right to life, to physical and moral integrity and to humane treatment in all circumstances. Under no circumstances shall any person be subjected to torture, to cruel, inhumane or degrading treatment."[1]

2.2 Law No. 90/036 of 10th August 1990 Relating to the Practice of Medicine in Cameroon

The 1990 Law relating to the Practice of Medicine in Cameroon is a key piece of legislation that plays a crucial role in safeguarding the right to health for the people of Cameroon. This law, enacted over three decades ago, has remained a cornerstone of the country's healthcare system, establishing a comprehensive regulatory framework to ensure the quality, accessibility and accountability of medical services.

One of the primary ways in which this law safeguards the right to health is by setting stringent standards for the practice of medicine in Cameroon.

In a bid to protect and safeguard the right to health of Cameroonians, some strict conditions have been imposed to govern the practice of medicine. Section 2 of the 1990 law imposes the following conditions:

"(1) Persons engaged in the practice of medicine in Cameroon shall be subject to registration with the Medical Association.

(2) However, physicians of foreign nationality who fulfil the following additional conditions may engage in the practice of medicine in Cameroon;

- Nationals of a country with a reciprocity agreement with Cameroon;

- Physicians who have not been struck off the roll in their countries of origin or in any other country where they had practiced medicine;

- Physicians recruited on contract or under a co-operation agreement exclusively for the Administration, a religious body or benevolent Non-Governmental Organization (NGO).

- Physicians serving in an approved private undertaking."[2]

Furthermore, in a bid to strictly govern the practice of medicine by private individuals, special conditions have been imposed by the 1990 law. Section 5 of the law states that:

"(1) The practice of medicine on a private basis shall be subject to an authorization issued by the Council of the Association under the terms and conditions laid down in this law.

(2) The Council of the Association shall also rule on applications for change of professional domicile or place of activity and resumption of activity after interruption following a disciplinary measure under conditions laid down by regulation.

(3) Authorizations granted by the Council of the Association must comply with the health map established by regulation.

Authorizations granted in violation of the health map shall be null and void."

Furthermore, in a bid to safeguard the right to health and ensure that patients are in safe hands, section 6 of the 1990 law stipulates that:

"Persons engaged in the practice of medicine on a private basis shall be subject to the following conditions:

- be of Cameroonian nationality and enjoy their civic rights;

- be registered with the Medical Association;

- must have completed five years of effective practice in a public service or a private body within the national territory or abroad;

- produce a letter of discharge where they are gainfully employed or assist a colleague who is practicing on a private basis;

- be of good conduct;

- produce an insurance policy covering occupational hazards;

- must have paid all their contributions to the Association."[3]

More so, in a bid to protect the right to health, certain conducts have been designated as unlawful within the context of medical practice. Section 16 of Law No. 90/036 of 10th August 1990 relating to the Practice of Medicine in Cameroon makes provision for what amounts to the unlawful practice of medicine. Section 16 states that:

[1] Preamble, paragraph 17 of the Preamble, Law No. 96/6 of 18 January 1996 as amended and supplemented by Law No. 2008/001 of 14 April 2008 on the Cameroon Constitution.

[2] Section 2, Law No. 90/036 of 10 August 1990 Relating to the Practice of Medicine in Cameroon.

[3] Section 5, Law No. 90/036 of 10 August 1990 Relating to the Practice of Medicine in Cameroon.

"The following shall be guilty of unlawful practice of medicine:

(1) any physician who practices under an assumed physician name or who grants consultations in business premises where some of the apparatus he prescribes or uses are sold;

(2) any unauthorized person who, even in the presence of a physician, habitually or under supervision, provides diagnosis or treatment for diseases on a personal basis by consultation or by any other procedure;

(3) any physician who exercises his profession in violation of the provisions under section l above or who offers his assistance to persons who are not authorized to practise;

(4) any physician who exercises his profession while on temporary or permanent suspension."[1]

Finally, in a bid to protect the right to health of all Cameroonians, sanctions have been provided for persons who engage in unlawful medical practice. Section 17 states that:

"(1) Without prejudice to the application of more severe administrative, disciplinary or penal sanctions, any person found guilty of unlawful practice of medicine shall be punished with imprisonment of from 6 (six) days to 6 (six) months or with fine of from 200 000 (two hundred thousand) to 2 000 000 (two million) francs or with both such imprisonment and fine.

(2) The court may, where applicable rule that the equipment used in the commission of the offence be confiscated and the establishment be closed.

(3) Any person who violates the provisions of this law shall cease his activity with immediate effect. Furthermore, the closure of his surgery establishment or clinic may be ordered by the Council of the Association, irrespective of any court judgment.[2]"

2.3 Law No. 95/08 of 30th January 1995 Relating to Radio Protection

The 1995 Law serves as a crucial legal mechanism for safeguarding the right to health in Cameroon, particularly in the context of radiation-related activities and exposure. This law establishes comprehensive regulations and guidelines to minimize the risks associated with ionizing radiation and ensures the well-being of the Cameroonian populace.

One of the primary objectives of this law is to protect the public, workers and the environment from the harmful effects of ionizing radiation. It does so by setting strict standards and requirements for the use, storage, transportation and disposal of radioactive materials and sources.

Article 1 of the 1995 law stipulates that:

"(1) The purpose of this law shall be to ensure the protection of man and his environment against the hazards that may result from the use of one or several sources of ionizing radiation, the use of a radioactive substance or the exercise of an activity that involves exposure to radioactivity.

(2) It shall govern the use of radioactive substances and energy for peaceful purposes, in the general interest."[3]

Furthermore, article 3 of the 1995 law enumerates the activities subject to the regulation of the law. Article 3 states that:

"(1) The activities targeted by this law shall be all those relative to the cycle of nuclear fuel and, particularly, the exploration and extraction of uranium ore and thorium, the acquisition, handling, production, transfer, processing, use, stocking, conveyance, importation of radioactive substances and radioactive sources as well as the installation of nuclear devices and equipment.

(2) These activities shall be subject to a prior authorization issued in accordance with terms and conditions laid down by statutory instruments, when a net positive benefit in the public interest can be derived from them, pursuant to the provisions of Section 2 above."[4]

In a bid to protect Cameroonian's right to health, sanctions have been imposed on whoever without authorization carries out radiation activities which tend to affect human health. Article 7, 8 & 9 clearly state that:

"Article 7: Whoever causes the exposure to ionizing radiation or a nuclear accident through imprudence or negligence, shall be punished with imprisonment for from five (5) to twenty (20) years and with a fine of from two hundred

[1] Section 16, Law No. 90/036 of 10 August 1990 Relating to the Practice of Medicine in Cameroon.

[2] Section 17, Law No. 90/036 of 10 August 1990 Relating to the Practice of Medicine in Cameroon.

[3] Article 1, Law No. 95/08 of 30 January 1995 Relating to RadioProtection.

[4] Article 3, Law No. 95/08 of 30 January 1995 Relating to RadioProtection.

thousand (200,000) to twenty million (20,000,000) francs CFA.

Article 8: Any person carrying out one of the activities referred to in Section 3 without prior authorization, shall be punished with imprisonment for from five (5) to ten (10) years and with a fine of from two hundred thousand (200,000) to twenty million (20,000,000) francs CFA.

Article 9: Whoever wilfully destroys all or part of a radioactive source or nuclear installation shall be liable to a death sentence."[1]

2.4 Law No. 2003/2006 of December 22, 2003 Governing Blood Transfusion

This legislation establishes a comprehensive regulatory framework to ensure the safety, quality, and availability of blood and blood products nationwide.

According to the aforementioned legislation, blood transfusion is to be prescribed by the doctor after taking into consideration the benefits to the patient and also the health risk involved. This is provided for by Article 7. This is to say, in a bid to ensure that the right to health is protected, the medical personnel needs to exercise due care to know the benefits and health risk involved in a blood transfusion to a patient before doing so, without which it will amount to medical negligence (breach of duty) if the patient is affected by that act.

"Article 8(1) of the said law goes further to say that: every blood transfusion act must be carried out with a clear consent, be it oral or written by the receiver or his or her legal representative, without which such act is a breach of duty. In case where the patient is unable to express his consent, the doctor will take a decision in the interest of the latter.

(2) When the patient is not able to express his or her consent, the doctor will take a decision in the patient's interest."[2]

Pursuant to article 9, the blood to be transfused must be submitted to all necessary screening and verification to confer to him (the patient) all the necessary characteristics and maximum security.[3]

Article 13 of the same law states that "anyone who takes blood samples out of a specialized and recognized structure or anyone who is not a doctor or assisted by a doctor, possess the act prescribed by the present law, shall be liable to an prison term of from 6 months to 2 years and with a fine of from one hundred thousand (100.000) to five hundred thousand (500.000) francs or one of these two penalties only. Same applies to any one being competent and exercising or practicing in a recognized structure.[4]"

In a bid to protect the right to health, the 2003 law imposes sanctions on persons who violate the rules governing blood transfusions in Cameroon. Article 15(1)-(3) stipulates that:

"(1) Any person who, having authority and working in an approved structure, collects blood without the consent of the donor is liable to the penalties of article 280 of the penal code.

(2) Any person who knowingly, in the course of taking blood, causes the donor injury, illness or incapacity to work, is punishable with the penalties as provided under Articles 277 and 279 of the Penal Code.

(3) In the event of death of the victim following the blunders and acts referred to in paragraph (2) above, the penalties applied to their perpetrator are those of article 278 of the penal code."[5]

Furthermore, pursuant to article 16 of the 2003 Law, any person who, by carrying out a blood transfusion, causes harm to others through clumsiness, inattention, imprudence or non-compliance with work is liable to the sanctions as provided for in articles 277 and 280 of the penal code.[6]

2.5 Law No. 2016/007 of July 12th, 2016 on the Penal Code

The penal code plays a crucial role in the protection of the right to health in Cameroon through several of its provisions. Firstly, Section 289 of the penal code stipulates that:

"(1) Whoever by lack of due skill, carelessness, rashness or disregard of regulation causes another's death or such harm, sickness or

[1] Article 7, 8 & 9, Law No. 95/08 of 30 January 1995 Relating to Radioprotection.

[2] Article 8(1) & (2), Law No. 2003/2006 of December 22, 2003 Governing Blood Transfusion in Cameroon.

[3] Article 9, Law No. 2003/2006 of December 22, 2003 Governing Blood Transfusion in Cameroon.

[4] Article 13, Law No. 2003/2006 of December 22, 2003 Governing Blood Transfusion in Cameroon.

[5] Article 15(1)-(3), Law No. 2003/2006 of December 22, 2003 Governing Blood Transfusion in Cameroon.

[6] Article 16, Law No. 2003/2006 of December 22, 2003 Governing Blood Transfusion in Cameroon.

incapacity as is described in section 277 or 280 shall be punished with imprisonment for from three (3) months to five (5) years or with fine of from ten thousand (10.000) to five hundred thousand (500.000) FCFA or with both such imprisonment and fine.

(2) Where such harm, sickness or incapacity as is described in Sections 277 or 280 is caused by an offence against section 227 or 228 (2) (a) or (b), the imprisonment shall be from 6 six(6) to twenty (20) years."[1]

Furthermore, Section 286 stipulates that:

"Sections 277 to 281 inclusive shall not apply to the professional services of any person duly authorized to render them, where performed with the consent either of the patient or of such person as may have custody of him:

Provided that where the patient is incapable of consent, his spouse may consent on his behalf, and where communication with the said spouse or person having custody is impossible, and without risk to the patient, consent shall not be necessary."[2]

The aforementioned provision safeguards the right to health in that it authorizes a medical personnel to carry out medical treatment without consent where the patient or his/her spouse is incapable of giving consent. This is in order to ensure that the health of patients is prioritized and not jeopardized.

2.6 Decree No. 83/166 of April 12th 1983 Establishing the Code of Medical Ethics in Cameroon

This decree was enacted in response to the need to regulate the medical profession and ensure that healthcare services are provided in an ethical and responsible manner. The code outlines the duties and obligations of medical practitioners, including the requirement to prioritize the well-being and interests of their patients. This is particularly important in the context of the right to health, as it helps to ensure that patients receive high-quality, comprehensive and non-discriminatory healthcare services.

The Code of medical ethics enumerates a multiplicity of ethical rules aimed at protecting the right to health, to which medical practitioners must conform. Some of these ethical principles include:

Section 1: which states that: Respect for life constitutes in every instance the primary duty of a doctor.[3]

Section 2 further stipulates that:

"(1) The doctor must treat all sick persons with the same diligence, whatever their status, nationality, religion, reputation and the feelings he may have concerning them.

(2) In no case shall the doctor exercise his profession under conditions pre-judicial to the quality of medical care and attention."[4]

Section 3 on its part provides that:

"(1) Whatever his official duties or special field may be, every doctor must, except in the case of force majeure, give help urgently to a sick person in immediate danger, unless he has ensured that other medical care likely to ward off the danger has been given to him.

(2) He may not leave his patients in the event of public danger, except upon an order issued in writing by the competent authority."[5]

Section 7 further stipulates that:

"The medical profession shall not be exercised like a trade. For this reason:

(a) Any form, direct or indirect, of publicity or advertisement, and any spectacular occasion concerning medical matters but not having exclusively a scientific or educational purpose shall be forbidden.

(b) The only observations which a doctor is authorized to enter on his prescriptions or in a year book are:

- those which facilitate his relations with his patients;

- such titles, duties, qualifications that are officially recognized and are related to the profession;

- scientific honours related to the profession.

(c) The only information that a doctor is authorized to put up on the door of his consulting room are the surname, names, titles, qualifications, the days, times for consultation and the floor, where applicable. Such information must be displayed with due

[1] Section 289, Law No. 2016/007 of July 12, 2016 on the Penal Code.

[2] Section 286, Law No. 2016/007 of July 12, 2016 on the Penal Code.

[3] Section 1, Decree No. 83/166 of April 12 1983 Establishing the Code of Medical Ethics in Cameroon.

[4] Ibid Section 2.

[5] Ibid Section 3.

restraint according to the custom of the liberal professions. The plate on which they are to be inscribed must not be larger than 25 cm by 30 cm. In the event of possible confusion, the medical association may require that first name(s) be mentioned."[1]

In addition, in a bid to protect the right to health, article 22 stipulates that:

"A doctor, from the moment he is called to give attention to a patient and agrees to do this, shall be bound: to give the patient all the necessary medical care withing his power, either personally or with the help of qualified third parties; to always act correctly and courteously towards the patient and to show himself sympathetic towards him."[2]

Section 23 on its part states that:

"(1) A doctor must always formulate his diagnosis with the greatest care, regardless of the time that this work may cost him.

(2) After having made his diagnosis and prescribed treatment, the doctor must endeavour to ensure that this treatment is carried out, especially if the patient's life is in danger."[3]

Section 24 proceeds to stipulate that:

"(1) A doctor must always prescribe treatment within the limits imposed by the conditions of the patients. He must in good faith not prescribe very costly treatment for a patient until the patient or his family have been informed of the sacrifices which this would entail and the benefit which they may derive from it.

(2) A doctor must never give treatment to a patient with a view to profiting therefrom."[4]

A perusal of all the aforementioned provisions of the 1983 decree establishing the code of medical ethics reveals that the decree contains a multiplicity of obligations bestowed upon medical practitioners, to ensure that they exercise their profession with dignity and professionalism, an outcome which will be liable to protecting the right to health in Cameroon.

3. The Role Played by State Courts in Combating Medical Negligence in Cameroon: A Review of Selected Case Laws

Cameroonian courts have been a vital instrument utilized by the State in the fulfilment of this goal, through the prosecution of some medical negligence-related cases in order to deter medical professionals from further engaging in acts of negligence which have devastating effects on the right to health. Some of these cases are analyzed in the subsequent paragraphs.

Nsame Emmanuel v. the People[5]

This case involved medical negligence resulting in severe injury to a five-day old baby. In this case, the leg of a five-day old baby was amputated as a result of the negligent act of a medical doctor at the Saint John Baptist Health Center in Ndop. While at the hospital, the said medical doctor discovered that the leg of the baby had suddenly became swollen as a result of unknown causes. In an attempt to solve the problem, the baby was facing, the medical doctor bandaged an ice block to the leg of the baby overnight. At 3am, the child started crying uncontrollably, which prompted the defendant to check on the condition of the baby, upon which he realized that the ice block had melted. The defendant upon realizing that the ice block had melted collected more ice blocks and further bandaged them to the leg of the child. The following morning, it was discovered that the state of the child's leg had worsened and had become even more swollen than it was the previous day. At the Ndop district hospital, it was determined that the child's leg had been severely damaged and had to be amputated. The defendant was found liable for medical negligence by the North West Court of Appeal and convicted accordingly.

Agborock Lydienne v. Dr. Nwaobi Romanus & St. John of God Hospital Nguti[6]

In this case, a medical doctor at St. John of God Hospital Nguti, named Nwaobi Romanus was found guilty of medical negligence as he failed to exercise the ordinary skill of an ordinary competent man exercising the duty of a medical doctor. The medical doctor in this case conducted an operation (surgery) and negligently left a swab inside the body of the patient. In fact, as a result of the operation,

[1] Section 7, Decree No. 83/166 of April 12 1983 Establishing the Code of Medical Ethics in Cameroon.

[2] Section 22, Decree No. 83/166 of April 12 1983 Establishing the Code of Medical Ethics in Cameroon.

[3] Section 23, Decree No. 83/166 of April 12 1983 Establishing the Code of Medical Ethics in Cameroon.

[4] Section 24, Decree No. 83/166 of April 12 1983 Establishing the Code of Medical Ethics in Cameroon.

[5] Suit No. CANWR/ICC/5C/2011 (Unreported).

[6] Suit No. HCK/14/2001-2002 (Unreported).

severe bleeding occurred, prompting the surgeon to make use of swabs to control the bleeding, which he eventually left in the body of the patient. The negligent act of the medical doctor resulted in severe consequences on the patient, which began to manifest a few hours after the surgery was over. The court in this case held that the medical doctor had been negligent and that had the accused exercised the care and skill reasonably expected of a surgeon, he would not have injured the patient. The court's judgment finding the accused guilty and punishing him accordingly, is vital in that it serves as a vital tool for deterring medical doctors/surgeons from such negligent behavior, thereby encouraging them to exercise due skill and due diligence in the course of their profession.

The People & 2 Ors v. Ndeumeni Noubevan Charles Dechateau and Ministry of Public Health[1]

In this case, the issue before the Littoral Court of Appeal was that of medical negligence manifested in the form of misdiagnosis resulting in substandard treatment of a patient. The patient in this case visited a hospital in Douala, revealing to the doctor how she felt. The medical doctor on his part, as a result of negligence, failed to make accurate and appropriate diagnosis of the patient's condition which resulted in inadequate treatment. Based on the fact that misdiagnosis is one of the most serious forms of medical negligence in contemporary societies, the Court of Appeal of the Littoral Region held the defendant liable for misdiagnosis of the patient's condition, resulting in substandard treatment of the said patient. Just like the decisions in the preceding cases, the decision of the Littoral Court of Appeal is relevant in that it served as a vital tool for deterring medical doctors from negligent behaviors, thereby encouraging them to exercise due skill in the course of their profession.

The People of Cameroon v. Dr. Eban Kingsley Barueta[2]

In this case which concerns medical malpractice, the Fako High Court convicted and sentenced Dr. Eban Kingsley Barueta to 18 years imprisonment and to pay cost of 522.280Fcfa for rape under section 298(a)(b) as read with section 131 of the penal code. In fact, Dr. Eban Kingsley was at the time of the offence, the Director of the Muyuka District Hospital while the victim, Fon Blessed Yencheck, was a volunteer nurse at the said hospital. In this case it is alleged that in the morning of Friday 21st May 2021, the victim of the offence, Fon Blessed Yencheck, a volunteer nurse at the Muyuka Distric Hospital, arrived the hospital in the morning to carry out her duties as volunteer worker. The accused, Dr. Eban Kingsley Barueta who was the Director of the said hospital, sent one doctor to invite her to attend the rounds of interned patients piloted by the accused. The victim assisted at the rounds as requested. The victim was taken aback by the accused's harsh attitude towards the patients, which attitude instilled fear of the accused in the victim. After the rounds, the accused invited the victim into his office, offered her a seat and informed her that he wanted to teach her something. The accused then instructed the victim to lie on the bed, an order she immediately obeyed because of fear. At this juncture the accused inserted his finger into the victim's vagina. Thereafter the accused suddenly asked the victim to leave his office, with firm instructions that she should return in ten minutes with a book. Upon her return, the accused instructed the victim to remove her pant, asking her not to be afraid as this was his routine procedure with all new internes, which instructions the victim obeyed out of fear of the accused. The victim lay on the bed face upwards and descended her body as instructed by the accused. The victim was gripped by fear to the extent that she could barely look at the accused's face. Then suddenly the victim felt the accused's penis inside her vagina. The penetration caused the victim severe pains which made her push the accused off her body as she scrambled off the bed. The accused gave the victim some tissue to clean her vagina, which exercise left blood stains on the tissue. The accused asked the victim to throw the tissue inside a trash can in the accused's office, and then pushed her out of his office with firm warning not to inform anyone of the act. Upon a complaint lodged against him, the accused was investigated, tried, convicted and sentenced as mentioned above.

The People of Cameroon v. Dr. Chuisseu John Ngongang[3]

In this case, the deceased, one Tabot Getrude

[1] Arret No. 35/CRIM of 15th June 2011 (Unreported).

[2] *Suit No. HCF/149CF/2021*

[3] CFIB/200F/2024

Achale, a woman aged 31 and midwife at C.M.A., a health facility at Mutengene, got pregnant sometime in March 2023. Her antenatal consultation at the C.M.A. Hospital Mutengene where she was working, showed that she had multiple fibroids, making her pregnancy a delicate and risky one. As a result of the C.M.A. Hospital's inadequate medical facility to handle surgeries of that magnitude, the deceased was referred to the Buea Regional Hospital which had the facility and specialists competent to carry out such delicate cesarian sessions to remove the baby and do the necessary myomectomy to remove the fibroids in the deceased's womb in order to save her life and that of her baby.

Shortly after the referral, the deceased later contacted the Accused, a General Practitioner working with the Sub Divisional Hospital Muea, who was not a specialist in that field, as he was neither a surgeon nor a gynaecologist, but who went ahead to programme her for a cesarian session on the 18th day of November, 2023.

Before the surgery, the accused had no proper antenatal and gynaecological history of the deceased, as he relied on the ultra sound test conducted on the latter two months before the surgery, to carry out the operation. Thus, no operative test was conducted on the deceased at the Muea Hospital prior to the surgery. The accused had no knowledge of the exact number and sizes of the fibroids in the womb of the deceased before the operation. There was no blood for transfusion in case of need before or after the surgery. The accused carried out the operation without any specialist nor any other doctor in that hospital. Both the cesarian session and the myomectomy were carried out on the same day against medical advice. Even though the accused succeeded, five minutes into the cesarian session, to bring out the baby, he proceeded immediately to the myomectomy by tying the base of the womb in a bid to reduce bleeding so as to extract the fibroids individually, a process which took five hours. In that light, the accused who had not done a proper diagnosis, was surprised of the number and sizes of the fibroids in the womb of the deceased after she was opened up. The up shoot of that discovery was that the sutures provided for that operation were insufficient thus prompting the accused to send for more via PW1 while the deceased was still under surgery in the theatre room. Since the operation took a longer time than expected, the spinal anesthesia that was administered on the deceased at 7.30 a.m. got expired at 12.00 noon and the deceased started crying of pain while the myomectomy was ongoing. Even though a light anesthesia was administered on her to calm her pains, the deceased started bleeding and shortly after, her vital signs became abnormal. In reaction the accused opted for blood transfusion but because there was no blood bank, he immediately ordered for blood, which came some minutes after the deceased had bled almost to death. When the blood finally came, the deceased passed away in the process of transfusion.

At the end of a trial conducted by the Court of First Instance Buea after a complaint and an investigation, the accused was held liable for incompetence and medical negligence, found guilty and convicted for unintentional killing under section 289(1) of the Cameroon Penal Code. He was sentenced to three (03) months imprisonment and to pay a fine of three hundred thousand (300.000) Fcfa and also to pay cost of one hundred and thirty-eight thousand, two hundred and sixty (138.260) FCFA.

The Case of Sergeant Mouyakan A Mougnol Willy[1]

One of the outstanding cases of medical negligence which has been taken to the Military Court is that of Sergeant Mouyakan A. Mougnol Willy who passed away on April 14th 2022. The Rapid Intervention Batallion (BIR) soldier was transferred from the Man O War Bay hospital Limbe to the Douala General hospital before being taken to IDIMED Clinic in Douala for neurosurgery. There, he was administered a double dosage (overdose) of anesthesia during the surgery and he never woke up. The anesthetist allegedly failed to take proper medical history leading to the fatal overdose, and left the patient unattended in the ICU after surgery. The family took the matter to the Douala Military Court against IDIMED clinic, and the anesthetistt.

Even though not all of the medical negligence and malpractices cases have been taken to court, they have however been reported. The following are examples of such.

Ilyana Tresor's[2]

A 5-year-old girl died at the Polyclinique

[1] Cameroon Concord News (2022)

[2] Journal du Cameroun (2020)

Archange in Douala due to an inadequate dose of anesthesia. The anesthetist mistakenly assumed she was 10 years old, highlighting the need for accurate patient assessment.

Dr. Jerry Esua's Case[1]

A doctor in Kumba was arrested and detained following the death of a premature baby. The doctor claimed he was assaulted by the father of the deceased and was only detained after calling the police.

Martina Nfor's Case[2]

A woman died after undergoing a cesarean section at the Buea Regional Hospital. The family alleged that the hospital staff was negligent, leading to the mother's death.

Ngum Victor's Case[3]

A man lost his leg due to alleged medical negligence at the Douala General Hospital. The hospital allegedly failed to provide timely and adequate care, resulting in amputation.

Nformi Emmanuel's Case[4]

A patient died after being administered the wrong medication at the Bamenda Regional Hospital. The incident highlights the need for proper medication management and patient safety protocols.

Atanga Henrietta's Case[5]

A woman suffered complications after a botched surgery at a private clinic in Yaoundé. The clinic allegedly lacked proper equipment and expertise, leading to the patient's suffering.

Tchouatchouang Yves' Case[6]

A patient died due to alleged medical negligence during surgery at the Yaoundé University Teaching Hospital. The family claimed that the hospital staff was incompetent and negligent.

Manka Elsie's Case[7]

A woman suffered burns during a medical procedure at a hospital in Douala. The incident highlights the need for proper equipment maintenance and staff training.

Foncha Andrew's Case[8]

A patient died after being discharged prematurely from the Bamenda Regional Hospital. The family alleged that the hospital staff failed to provide adequate care and monitoring.

Nkwenti's Case[9]

A patient suffered permanent disability due to a delayed cesarean section at a hospital in Yaoundé. The delay allegedly resulted from hospital staff negligence.

Ebenezer's Case[10]

A child died due to alleged medical negligence during a surgical procedure at a hospital in Douala. The family claimed that the hospital staff was incompetent.

Nforneh's Case[11]

A woman suffered complications after a botched abortion at a private clinic in Bamenda. The clinic allegedly lacked proper equipment and expertise.

Tanyi's Case[12]

A patient died due to alleged medical negligence during treatment at a hospital in Kumba. The family claimed that the hospital staff was negligent and incompetent.

Mbuh's Case[13]

A patient suffered permanent disability due to a medical procedure at a hospital in Yaoundé. The incident highlights the need for proper patient care and monitoring.

Njoh's Case[14]

A patient died due to alleged medical negligence during surgery at a hospital in Douala. The family claimed that the hospital staff was negligent.

Nkfusai's Case[15]

A woman suffered complications after a cesarean section at a hospital in Bamenda. The incident highlights the need for proper postpartum care.

1 Case The Guardian Post (2020)
2 Cameroon Tribune (2018)
3 Le Messager (2019)
4 The Post Newsline (2020)
5 Cameroon Info (2019)
6 La Nouvelle Expression (2020)
7 The Guardian Post (2020)
8 The Post Newsline (2020)
9 Cameroon Tribune (2019)
10 The Guardian Post (2021)
11 The Guardian Post (2020)
12 Cameroon Info (2020)
13 The Post Newsline (2020)
14 The Post Newsline (2020)
15 The Herald Newspaper (2021)

Fopa's Case[1]

A patient died due to alleged medical negligence during treatment at a hospital in Yaoundé. The family claimed that the hospital staff was incompetent.

Tamen's Case[2]

A patient suffered permanent disability due to a delayed diagnosis at a hospital in Douala. The delay allegedly resulted from hospital staff negligence.

Keme's Case[3]

A woman suffered complications after a botched surgery at a private clinic in Yaoundé. The clinic allegedly lacked proper equipment and expertise.

These cases demonstrate the need for improved healthcare standards, accountability, and patient safety protocols in Cameroon.

Although the work is restricted to Cameroon, inspiration is also drawn from other jurisdictions to support the arguments in this write-up. We shall therefore cite some foreign cases on medical negligence/malpractice to buttress Cameroon cases.

Gerber v. Pines[4]

In this case, in giving treatment by injection, a needle was broken and left in the patient's body and the patient was not informed and this resulted in the patient suffering pain and injury as an operation had to be carried out to remove the broken needle. The doctor was found guilty of medical negligence.

The Death of Michael Jackson

The death of popular musical Icon Michael Jackson in 2009 brought worldwide attention to the issue of medical negligence. Michael Jackson's personal physician, Dr. Conrad Murray was found guilty of involuntary manslaughter for negligently administering a lethal dose of the anesthetic propofol on Michael Jackson which caused his death. Dr. Murray, a cardiologist based in Houston, received a monthly payment of $150.000 for his role as Michael Jackson's personal doctor during the rehearsals in Los Angeles for the *This Is It* concert series. During the criminal trial, it was revealed that Dr. Murray spent at least six nights a week with Jackson and was frequently implored by the singer, who suffered from chronic insomnia, to administer sleep-inducing medication. Jackson specifically sought only propofol, a potent surgical anesthetic, which he preferred over other strong sedatives. Evidence presented in court suggested that it was propofol, combined with other unrequired medications which the doctor administered in Jackson's system that was primarily responsible for his death on June 25th, 2009. Surviving members of Michael Jackson's family filed a civil death lawsuit against concert promoter AEG Live. They alleged that AEG Live was negligent in hiring Dr. Murray and should be responsible for Jackson's death. The family argued that AEG Live pressured Dr. Murray to prioritize Jackson's ability to perform over his health and wellbeing. The trial which took place in 2013, lasted for several months and included extensive testimonies and evidence. Ultimately, the jury found that while AEG Live did hired Dr. Murray, he was not unfit or incompetent for the work for which he was hired, absolving the company of liability in Jackson's death, as it was Dr. Murray's personal medical negligence that caused Michael Jackson's death.

The Plight of Julie Andrews

A world renowned actress, Julie Andrews, perhaps best known for her roles in Mary Poppins and the Sound of Music, underwent surgery in 1997 at Mt. Sinai Hospital to remove noncancerous nodules from her throat. Tragically, the surgery led to permanent damage to her vocal cords, effectively ending her singing career. Julie Andrews cried out saying "Singing has been a cherished gift and my inability to sing has been a devastating blow to me." Julie filed a medical malpractice lawsuit against the Doctors involved, alleging that the operation was botched, leaving her with hoarseness, permanent vocal damage and other complications. The lawsuit was settled for an undisclosed amount in 2000.

The Death of Stella Abebe Obasanjo

Another pathetic situation of medical negligence is the death of Stella Abebe Obasanjo, the wife of one time President of Nigeria, Olusenjo Obasanjo. She died on 23rd October, 2005 at the age of 59, from surgical complications, that is, complications of cosmetic surgery at a private health clinic in Puerto Banus, Marbella, Spain,

[1] Cameroon Info (2021)

[2] The Times Newspaper (2022)

[3] The herald (2021)

[4] (1933) 79 SJ 13

caused by the negligence of the doctor. The physician had misplaced a tube designed for a liposuction procedure into Stella Obasanjo's abdominal cavity. As a result, she sustained a punctured colon and lacerated liver during the surgery and died two days after the surgery. In a law suit that President Obasanjo ordered, the doctor was held liable for medical negligence and made to pay damages and his licence withdrawn for time.

4. Conclusion

Medical negligence has in contemporary times dominated discourses on human rights, specifically the right to health at the international, regional and domestic scenes. The increased zeal of the international community to address this cankerworm has led to the adoption of diverse measures which have over the years contributed to addressing the issue to a notable positive extent.

Even though the existing legal and institutional regimes in Cameroon have continuously provided sanctions for perpetrators in an attempt to combat and eradicate medical negligence in Cameroon, the attainment of a society absolutely void of instances of medical negligence hitherto remains an expectation. This has been manifested in several instances highlighting the voluntary and involuntary violation of legislation governing the practice of medicine, which contributes to further instances of medical negligence in Cameroon. This study has revealed that some of the reasons for the persistence of medical negligence in *i*nclude: the existence of weak Cameroon despite the existence of a legal and institutional framework regulatory mechanisms; the inefficient enforcement of existing laws; difficult access to judicial redress; Cameroon's limited technological capacity, amongst others.

Nevertheless, considering the increased efforts made towards the fight against medical negligence, which is manifest in the increase in interests to curb the rate of violation of medical protocol resulting in damage to patients, and the increase in the prosecution and punishment of perpetrators of acts or omissions qualified as medical negligence, it would not be wrong to say that the future holds an even more safe and healthy Cameroonian society, where health and medical safety protocol will be upheld by medical personnel, characterised by the latter actively engaging in the fight against medical negligence through the exercise of due diligence in their course of the exercise of their profession.

5. Recommendations

In view of the challenges faced in the fight against medical negligence in a bid to promote the right to health in Cameroon, a number of measures are worth proposing to strengthen the fight against medical negligence and facilitate the realization and protection of the right to health. The researcher therefore advances the following recommendations: The Strengthening of Regulatory Bodies/Mechanisms especially the courts in Cameroon.

The Strengthening of Regulatory Bodies/Mechanisms

The existence of weak regulatory mechanisms has been identified as a major challenge faced in the fight against medical negligence in Cameroon. In a bid to address this hurdle, the researcher recommends that existing regulatory bodies such as the Cameroon Medical Council and MINSANTE should be strengthened and empowered with the requisite funding and technological resources necessary for effectively monitoring medical practice in Cameroon. For example, the Cameroon Medical Association should be empowered to oversee the process of licensing of medical professionals and carry out independent investigations to ensure that only qualified and licensed individuals are engaged in the practice of medicine in Cameroonian.

Also, considering that the members of the Cameroon Medical Association are doctors/medical personnel, there is often a tendency for them to protect their colleagues when complaints are made against them. In a bid to prevent this situation and safeguard the right to health in Cameroon, the researcher recommends that an independent department, to be made up of not only the medical personnel, be created in the Ministry of Public Health to monitor and supervise the activities of the Cameroon Medical Association vis-à-vis the complaints they receive, to ensure that no bias exists when handling complaints against medical personnel. The researcher recommends that the said department be empowered with the authority to sanction and suspend members of the Cameroon Medical Association who fail to discharge their obligations with integrity and dignity. Such a step will be vital in that it will promote transparency and accountability not only within the Cameroon Medical Association,

but within medical practice as a whole- an outcome which will be liable to strengthening the protection of patients thereby facilitating the realisation of the right to health in Cameroon.

References

Campbell. D. (2011). Hospital Patients Complain of Rude Staff, Lack of Compassion and Long Waits. *The Guardian*. Available online at: https://www.theguardian.com/society/2011/feb/23/hospital-patients-rude-staff-long-waits. Accessed on January 28, 2024.

Chris Turner. (n.d.). *Unlocking Torts,* 4th Edition. London: Routledge Publishing, p. 26.

E. Pierre Gould. (1937). The Defence of Medical Negligence. *Medico-Legal Criminological Review, 5*(2), pp. 191.

Ezinne Vivian & Chidinma Blessing Nwakoby. (2013). Medical Negligence in Nigeria. *Journal of Education, Humanities, Management & Social Sciences (JEHMSS),* pp. 7-28.

Guptha Jaiprakash. (2002). *Ethics and Law Controlling Medical Practitioners.* Available online at: https://www.aironline.in/legal-articles/Ethics%20and%20Law%20-Controlling%20Medical%20Practitioners. Accessed on January 17th, 2024.

Hassan King Obaro. (n.d.). Legal Imperatives of Medical Negligence and Medical Malpractice. Available online at: https://www.njmonline.org. Accessed on January 28, 2024.

Law No. 80/6 of 14 July 1980 to Regulate the Practice of Medicine in Cameroon; Law No. 80/7 of 14th July 1980 to Organize the Medical Association in Cameroon.

Michael A. Jones. (1996). *Medical Negligence.* London: Sweet & Maxwell, p. 29.

Oliver Wendell Holmes Jr. (1881). *The Common Law.* London: Macmillan.

Oseni T.I.A. (2019). Medical Duty of Care: A Medico-Legal Analysis of Medical Negligence in Nigeria. *American International Journal of Contemporary Research, 9*(1), pp. 56-63.

Paragraph 4 & 5 of the Preamble, Law No. 96/6 of 18 January 1996 as amended and supplemented by Law No. 2008/001 of 14 April 2008 on the Cameroon Constitution.

Preamble, paragraph 17 of the Preamble, Law No. 96/6 of 18 January 1996 as amended and supplemented by Law No. 2008/001 of 14 April 2008 on the Cameroon Constitution.

PIONEER
ACADEMIC PUBLISHING LIMITED

Studies in Law and Justice
ISSN 2958-0382
www.pioneerpublisher.com/slj
Volume 4 Number 3 June 2025

Legal Responses to Online Hate Speech in India: Evaluating Section 66A and the Supreme Court's Judgment in Shreya Singhal v. Union of India

Rahul D. Thakkar[1]

[1] Jamia Millia Islamia University, New Delhi, India
Correspondence: Rahul D. Thakkar, Jamia Millia Islamia University, New Delhi, India.

doi:10.56397/SLJ.2025.06.03

Abstract

This paper critically examines India's legal responses to online hate speech through the lens of Section 66A of the Information Technology Act, 2000, and the landmark Supreme Court judgment in *Shreya Singhal v. Union of India* (2015). By tracing the evolution of Section 66A from its enactment to its judicial invalidation, the study highlights how vague legal provisions have been employed to suppress dissent in the digital space. The judgment in *Shreya Singhal* marked a doctrinal shift in Indian free speech jurisprudence by introducing constitutional tests of proportionality, precision, and incitement thresholds. Yet, post-judgment developments reveal persistent regulatory gaps, including the continued application of the repealed law and the emergence of executive-led content regulation under the IT Rules 2021. This paper argues for a reimagined legal framework grounded in rights-based, transparent, and procedurally robust safeguards that respect the normative centrality of freedom of expression in India's digital democracy.

Keywords: Section 66A, online speech, Shreya Singhal, hate speech regulation, Indian Constitution, digital censorship, IT Rules 2021

1. Introduction

The rapid expansion of internet access and social media platforms in India over the past two decades has dramatically reshaped the public sphere, bringing previously marginal voices into national discourse. With over 850 million internet users as of 2024, India hosts one of the largest digital populations globally, and online spaces—particularly Facebook, WhatsApp, Twitter (now X), and YouTube—have emerged as critical arenas for political debate, protest mobilization, and cultural expression. Yet this digital empowerment has also intensified challenges around hate speech, misinformation, and incitement, sparking heated debates over the proper limits of free expression in a democratic society.

India's Constitution enshrines freedom of speech and expression as a fundamental right under Article 19(1)(a), subject to reasonable restrictions outlined in Article 19(2), including those related to public order, decency, morality, and incitement to offenses. However, the interpretation of "reasonable" in a digital context has proven contentious. Unlike traditional speech, online communication is

instantaneous, transregional, and algorithmically amplified, making harmful speech not only more visible but more virulent in effect.

The state's legal response to this transformation has oscillated between protectionist paternalism and coercive censorship. Legislators and enforcement agencies have often invoked vague or broad statutory language to regulate online content, frequently under the guise of preventing unrest, protecting sentiments, or combating threats to national security. Critics argue that such legal instruments often blur the line between hate speech and political dissent, allowing the state to suppress criticism under pretexts of law and order.

This tension came to a head in the early 2010s with the proliferation of arrests under Section 66A of the Information Technology Act, 2000, a provision criminalizing online communication deemed "grossly offensive" or "of menacing character." The law was widely applied against students, journalists, satirists, and activists, fueling accusations of authoritarian overreach. Its enforcement triggered alarm across civil society, culminating in judicial intervention in the landmark Shreya Singhal v. Union of India case.

Thus, any analysis of India's legal response to online hate speech must begin by acknowledging the triangular conflict between:

- Technological acceleration of speech dissemination
- The democratic imperative of free expression
- The state's attempt to regulate the digital sphere through statutory authority

The story of Section 66A, its downfall, and the lingering regulatory vacuum left in its wake serves as a key episode in India's ongoing attempt to define the constitutional limits of digital speech in a time of unprecedented communicative flux.

2. Section 66A of the IT Act: Text, Application, and Controversy

Enacted through an amendment to the Information Technology Act in 2008, Section 66A was designed ostensibly to address the growing misuse of digital platforms to spread harmful or offensive content. The provision criminalized the sending of information via a computer resource or communication device that was *"grossly offensive," "menacing in character,"* or that caused *"annoyance," "inconvenience,"* or *"insult."* Convictions could lead to up to three years of imprisonment and fines.

At a textual level, the provision was notable for its vague and subjective terminology, lacking clear definitions or thresholds for what constituted "gross offensiveness" or "annoyance." The provision's open-ended language—with no requirement for intent, harm, or public order disruption—stood in stark contrast to constitutional jurisprudence that requires speech-restrictive laws to be narrowly tailored and proportional.

In practice, Section 66A became a widely used tool for suppressing dissent and curbing legitimate speech. Between 2009 and 2015, numerous citizens were arrested for online posts criticizing politicians, questioning government policies, or sharing satirical content. Prominent cases include:

- Shaheen Dhada and Rinu Srinivasan (2012): Arrested in Maharashtra for Facebook posts questioning a citywide shutdown following the death of a political leader.
- Ambikesh Mahapatra (2012): A professor detained for forwarding a political cartoon via email.
- Cartoonist Aseem Trivedi (2012): Prosecuted for posting cartoons satirizing corruption.

According to data compiled by the Internet Freedom Foundation and NCRB records, over 3,000 cases had been filed under Section 66A by 2014. However, few of these resulted in convictions—highlighting its instrumental role in harassment and pretrial punishment, rather than actual legal resolution.

The public outcry intensified as civil society groups, legal scholars, and free speech advocates criticized the provision for enabling state-sponsored intimidation. The lack of judicial safeguards or statutory clarity gave law enforcement broad discretion to arrest individuals based on subjective offense, often triggered by political or religious sensitivities.

Further, the non-bailable and cognizable nature of the offense allowed for immediate detention without court approval, amplifying the chilling effect on digital speech. The constitutional

inconsistency of the law with Article 19(1)(a)—especially in terms of overbreadth and arbitrariness—formed the basis of legal challenges that culminated in *Shreya Singhal v. Union of India*.

In retrospect, Section 66A became emblematic of India's struggle to balance digital regulation with democratic accountability. Its trajectory from enactment to repeal reveals how legal instruments, when poorly crafted, can serve as vehicles of censorship rather than protection, underscoring the need for clarity, proportionality, and constitutional alignment in the governance of online expression.

3. *Shreya Singhal v. Union of India*: Constitutional Scrutiny and Doctrinal Shift

The landmark judgment in *Shreya Singhal v. Union of India* (2015) marked a watershed moment in India's digital free speech jurisprudence. Sparked by a series of publicized arrests under Section 66A of the Information Technology Act, the case was initiated through a Public Interest Litigation (PIL) by law student Shreya Singhal, challenging the constitutionality of the provision on the grounds that it violated Article 19(1)(a) of the Indian Constitution.

At the heart of the Court's deliberation was the tension between the state's obligation to maintain public order and the citizen's right to free expression in the digital realm. Section 66A, the petitioners argued, was vague, overbroad, and lacked proximate connection to any of the reasonable restrictions outlined in Article 19(2).

In a historic verdict, a two-judge bench of the Supreme Court (Justices J. Chelameswar and Rohinton Nariman) unanimously struck down Section 66A as unconstitutional in its entirety. The Court's reasoning centered on three key doctrinal developments:

(1) Vagueness and Overbreadth

The Court held that terms such as *"grossly offensive," "annoyance,"* and *"menacing in character"* were constitutionally void for vagueness. Such language failed to provide clear guidance to citizens and law enforcement alike, leading to arbitrary and subjective application. Citing U.S. jurisprudence (e.g., *Grayned v. Rockford*), the Court reiterated that vague laws have a chilling effect on legitimate speech and are therefore incompatible with fundamental freedoms.

(2) Distinction Between Discussion, Advocacy, and Incitement

Drawing from international free speech doctrine, the Court emphasized a tripartite framework:

- *Discussion* and *advocacy*, even if unpopular or offensive, are protected under Article 19(1)(a)
- Only *incitement to violence or public disorder* can be reasonably restricted

Section 66A, by criminalizing mere annoyance or offensive communication without reference to incitement or actual harm, failed this constitutional test.

(3) Proportionality and Lack of Nexus with Article 19(2)

The judgment asserted that a restriction on speech must have a direct and proximate link to the grounds enumerated in Article 19(2)—such as sovereignty, public order, or decency. Section 66A's broad sweep criminalized a range of expression without establishing such a nexus, rendering it disproportionate and excessive in scope.

The Court rejected the government's argument that the provision had a deterrent value against cyber threats, holding that no matter how laudable the goal, it cannot justify disproportionate means.

The judgment in *Shreya Singhal* not only invalidated a widely misused provision but also laid down a foundational jurisprudential framework for assessing future restrictions on digital speech in India. It reaffirmed that the internet is not an exception to constitutional protections and that legal instruments regulating speech must meet the highest standards of precision and necessity.

However, as later developments would reveal, the judgment's doctrinal clarity was not always matched by administrative enforcement, with police departments continuing to invoke Section 66A in thousands of cases even after its repeal—highlighting the gap between judicial articulation and regulatory practice, a theme explored in the following section.

4. Persisting Legal Gaps and Extra-Judicial Regulation Post-66A

Despite the categorical invalidation of Section 66A by the Supreme Court in *Shreya Singhal v. Union of India*, the implementation of the ruling has been erratic and incomplete, revealing structural deficiencies in India's

speech-regulatory ecosystem. The post-judgment period is marked by two troubling trends: the continued use of repealed legal provisions and the emergence of new, often opaque regulatory instruments that bypass traditional legislative scrutiny.

Continued Use of Section 66A in Practice

Multiple studies and Right to Information (RTI) disclosures have shown that Section 66A continues to be invoked in police reports, charge sheets, and even judicial orders years after it was struck down. According to a 2022 compliance report submitted to the Supreme Court by the People's Union for Civil Liberties (PUCL), over 1,000 cases invoking Section 66A were registered *after* the 2015 judgment, with arrests continuing as late as 2021.

This legal necromancy is attributable to:

- Lack of communication between central databases and district-level police forces
- Legacy case management systems in lower courts and law enforcement
- Ambiguity in new statutory replacements for cyber misconduct

The persistence of a "zombie law" reveals not merely bureaucratic inertia but a deeper issue: the fragility of judicial supremacy in regulatory practice, especially when executive agencies retain wide discretionary powers.

The Rise of Executive Rule-Making: IT Rules 2021

In the vacuum left by 66A, the Government of India introduced the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, under the IT Act. These rules empower the executive to:

- Demand content takedown within 36 hours
- Require social media platforms to appoint grievance officers and provide traceability of messages
- Subject digital news outlets and OTT platforms to a three-tier compliance mechanism

While the government frames the IT Rules as tools for ensuring accountability and public order, critics argue that they:

- Lack statutory backing from Parliament
- Blur the line between regulatory oversight and executive censorship
- Create chilling effects through the threat of criminal liability and platform delisting

Several High Courts, including those in Bombay and Madras, have stayed or severely restricted the enforcement of certain provisions, citing violations of constitutional safeguards and procedural fairness.

Platform Governance and the Rise of Soft Censorship

Alongside formal state action, content moderation is increasingly shaped by private platforms' compliance behavior. Social media companies—under pressure to conform to state demands—often pre-emptively remove content, suspend accounts, or adjust visibility metrics. This introduces a layer of informal censorship, where speech is regulated not by law but by opaque terms-of-service algorithms, with limited transparency or recourse for users.

In this regulatory blur, citizens face a fragmented speech regime: judicially protected in principle, but precariously governed in practice. The result is a chilling environment in which dissent is deterred not through statutory punishment but through a complex web of legal uncertainty, bureaucratic discretion, and platform compliance anxiety.

5. Reimagining Legal Safeguards for Online Speech in the Indian Context

The Indian experience with Section 66A, its judicial repeal, and the post-judgment drift into informal and extra-judicial content regulation raise urgent questions about the future of speech governance in a digital democracy. As the lines between state control, private moderation, and civic participation blur, the need for a principled, transparent, and rights-oriented legal framework becomes increasingly vital.

A future-facing speech regime must begin with the constitutional reaffirmation that freedom of expression is the rule, and restriction the exception—an inversion of the logic that has too often governed digital regulation in India. This demands a multi-pronged approach:

First, legislative clarity must replace executive ambiguity. Statutory definitions of "hate speech," "public order," and "incitement" must be precise, narrowly tailored, and context-specific, drawing on comparative jurisprudence and sociolinguistic research. Vague categories such as "offensive" or

"annoying" must be retired from all speech-related laws.

Second, any future regulations—be it content takedown rules or traceability mandates—must be grounded in due process and judicial oversight, not administrative discretion. Time-bound judicial review mechanisms, redressal portals, and transparency requirements for takedown orders should be codified by law, not merely platform policy.

Third, platform accountability should not mean coercive compliance. Regulation must ensure that global intermediaries operating in India uphold constitutional protections, including proportionality and non-discrimination, in their content moderation and algorithmic visibility practices. Independent audits and civil society oversight should be institutionalized.

Fourth, capacity-building within law enforcement and judiciary is essential. The continued application of repealed laws like Section 66A reflects not only institutional neglect but epistemic disempowerment. Training modules on constitutional rights, digital speech standards, and evidence-based policing must become integral to India's justice system.

Finally, and most crucially, legal reform must be animated by a normative vision: that online speech is not a risk to be mitigated but a right to be cultivated. In a deeply plural society, where social conflict often intersects with digital virality, the response to hate speech must go beyond censorship—it must include civic education, counter-speech promotion, and platform design that incentivizes dialogue over division.

The road beyond Section 66A is not just a matter of judicial compliance or legislative drafting. It is a democratic imperative—to ensure that India's digital spaces reflect not the anxieties of control, but the aspiration of a constitutional republic committed to liberty, dignity, and pluralism.

References

Basu, D. D. (2019). *Commentary on the Constitution of India*. New Delhi: LexisNexis.

Baxi, U. (2018). The Technological Republic: Platforms, Power, and Precarity. *Journal of Indian Law and Society*, *9*(2), 45–71.

Bhandari, A., & Nigam, A. (2020). *The Chilling Effect of India's IT Laws on Free Speech*. New Delhi: Internet Freedom Foundation.

Internet Freedom Foundation. (2021). *Zombie Provisions: Section 66A Post Shreya Singhal*. IFF Legal Brief Series.

Nariman, R. F. (2020). Judicial Review and the Protection of Free Speech in India. *National Law School Journal*, *32*(1), 3–19.

Rajagopal, K. (2022). Section 66A Still in Use Despite Supreme Court Verdict. *The Hindu*, July 2022.

Srivastava, A. (2021). The IT Rules 2021 and the Future of Online Speech Regulation. *Indian Journal of Law and Technology*, *17*(1), 61–83.

Supreme Court of India. (2015). *Shreya Singhal v. Union of India*, AIR 2015 SC 1523.

PIONEER
ACADEMIC PUBLISHING LIMITED

Studies in Law and Justice
ISSN 2958-0382
www.pioneerpublisher.com/slj
Volume 4 Number 3 June 2025

Mapping the Evolution and Practical Significance of Implied Terms in Contracts: Insights from the United Kingdom and Nigerian Legal Frameworks

Joseph Agburuwhuo Nwobike[1]

[1] Senior Advocate of Nigeria (SAN), Lead Partner, Osborne Law Practice, Nigeria
Correspondence: Joseph Agburuwhuo Nwobike, Senior Advocate of Nigeria (SAN), Lead Partner, Osborne Law Practice, Nigeria.

doi:10.56397/SLJ.2025.06.04

Abstract

Since *The Moorcock* case in 1889, the boat of implied terms has encountered storms and instability from scholarly debates. The key contentious issues orbit around the role of reasonableness, necessity, contract interpretation, and the continued relevance of the traditional tests. Historically, courts have used two main tests to imply terms into contracts: Lord Bowen's Business Efficacy Test and Lord Mackinnon's Officious Bystander Test. However, in *Belize Telecom Ltd* (2009), Lord Hoffmann opined that implying terms in contract is simply part of interpreting the contract as a whole, rather than applying the traditional tests: in response to this approach, a significant weight of judicial authority supports the view that *Belize* should not be perceived as a relaxation of the traditional tests towards implication of terms. While debates have continued on whether implied terms of fact should be a distinct process or simply part of contract interpretation, the UK Supreme Court in *Barton v Morris* (2023) held that if a term is sufficiently express, the doctrine of unjust enrichment and quantum meruit cannot be used to imply a term that possibly contradicts the express term—this is somewhat different from the position of law in Nigeria. This article is an illuminating synthesis of these differences: it charts a stable and harmonized course that smoothens out the rough patches which accrued over the years via intense legal polemics.

Keywords: implied terms, express terms, contractual interpretation, Lord Hoffmann, unjust enrichment, quantum meruit, Belize Telecom

1. Introduction: The Relevance of Implication of Terms in Fact

The *Black's Law Dictionary,* refers to a contract implied in fact as "a contract that the parties presumably intended as their tacit understanding as inferred from their conduct and other circumstances."[1] The relevance or necessity of 'implied terms' of facts in contracts draws from the regular practice of executing incomplete and indefinite contracts between business parties. For practical reasons, ranging from high costs of frequent (re)negotiations of

[1] (8th edn), p. 345.

contracts to future uncertainties about markets, businesspeople usually draft contracts to be sufficiently elastic to accommodate future but reasonably foreseeable facts which the parties could not have averted their minds at the onset (Ben-Shahar, 2004). The incomplete nature may or may not be a product of their common intention, but either reasons invites the court to decide on the extent it could save or kill the contract for lack of sufficient factual terms. Lord Bingham MR captured the forgoing challenge in *Philips Electronique Grand Public SA v British Sky Broadcasting Ltd*,[1] when he noted the difficulty of inferring with confidence what the commercial parties must have intended in a rather comprehensive contract because "… it may well be doubtful whether the omission was the result of the parties' oversight or of their deliberate decision; if the parties appreciate that they are unlikely to agree on what is to happen in a certain not impossible eventuality, they may well choose to leave the matter uncovered in their contract in the hope that the eventuality will not occur."[2] However, there is a limit to what could be inferred into a contract. As Lord Pearson echoed in *Trollope & Colls Ltd*,[3] "it must have been a term that went without saying, a term necessary to give business efficacy to the contract, a term which though tacit is part of the contract the parties made for themselves."[4]

Recently in *Betamax Ltd v State Trading Corporation*,[5] the Judicial Committee of the UK's Privy Council reiterated the age-old common law rule in relation to contract law that by nature, it bequeaths contracting parties with the power to make their own binding and enforceable rules subject to any applicable restrictions that anchor on law or public policy (Schwartz & Scott, 2003).[6] Based on the trite principle that the essence of contract is performance, common law courts tend to prefer an approach that salvages a wrecking contract for want of remediable facts, unless their incompleteness is too egregious and lacks fundamental terms upon which useful supplements could have been made. In furtherance to this objective of contract law, two observations may be noted. Firstly, where contractual terms/facts are incomplete or indefinite, courts would consider whether the incompleteness is too material as to result naturally to uncertainty and thus unenforceable.[7] Secondly, as the UK Supreme Court held recently in *Wells v Devani*,[8] it would further consider whether the incompleteness could be reasonably remedied through a gap-filling exercise that allows for the infusion of implied terms based on the presumed intention of the parties. In *Equitable Life Assurance Society v Hyman*,[9] Lord Steyn rightly observed that the implication of a term was "not critically dependent on proof of an actual intention of the parties." Nigerian courts have also adopted this type of reasoning: 'implied terms' is a regular staple in Nigerian contract law. In fact, a search with the keyword "implied terms of contract" in the database of Nigerian Weekly Law Reports—the country's most comprehensive database for law reports—produced more than a dozen Court of Appeal and Supreme Court decisions on the subject matter. Indeed, most of the cases reiterate the established positions of English case law on implied terms. For example, in *Union Bank of Nigeria plc v. Awmar Properties Ltd*,[10] the Nigerian Supreme Court (per Justice Rhodes-Vivour) held that "an implied term in a contract is a term necessary to give business efficacy to the contract. It is a term which though tacit, is part of the contract the parties made for themselves..." However, as can be seen in *British Movietonews Ltd*,[11] the eagerness of common law courts to imply terms into contracts to ensure their workability and performance should be qualified with their longstanding cautiousness not to intentionally make contracts for parties;[12] although as would be seen from Lord

[1] [1995] EMLR 472.

[2] Ibid, 481-482.

[3] *Trollope & Colls Ltd. v. North West Metropolitan Regional Hospital Board*, (1973) 2 All ER 260.

[4] Ibid, 268. Also see *Shell UK v. Lostock Garages* (1977) 1 All ER 481, Lord Denning MR at 488.

[5] [2021] UKPC 14.

[6] Earlier cases include Frost v Knight **(**1872**)** LR 7 Exch 111; Printing and Numerical Registering Co v Sampson (1875) 19 Eq 462.

[7] *Scammell and Nephew Ltd v Ouston* [1941] AC 251; *May & Butcher Ltd v The King* [1934] 2 KB 17.

[8] *Wells v Devani* [2019] UKSC 4**,** para 13.

[9] [2002] 1 AC 408, 459.

[10] *Union Bank of Nigeria plc v. Awmar Properties Ltd* (2018) 10 NWLR 64, 70. Also see *Multichoice (Nig.) Ltd v. Azeez* (2010) 15 NWLR (Pt.1215) 40, 42 and 51 (Court of Appeal).

[11] *British Movietonews Ltd v. London and District Cinemas Ltd* (1952) AC 166.

[12] See *Omega Bank v. O.B.C. Ltd*. (2005) 8 NWLR (Pt. 928) 547 (per Kutigi JSC, Nigerian Supreme Court).

Hoffmann's approach in *Chartbrook*, [1] enforcement or interpretation may include a broad scale rectification.

Whether or not an incomplete contract of parties resulted intentionally or otherwise, a court's power to intervene and cure the underlying defects is hardly in contention.[2] What is rather in contention, which by extension is the epicenter of this article is the methodologies common courts could employ to ascertain what terms should be implied in contracts. The article traces key judicial efforts, starting from *The Moorcock* case in 1889.[3] The case developed the 'business efficacy' test, which requires that an implied term of fact in contracts must be commercially efficacious as opposed to what a party unilaterally contends which may be commercially insensible or inefficacious.[4]

The challenge with the business efficacy test lies on its wide spectrum of subjective meanings, given that its determination may be derived from a party's unilateral (ambitious or restrictive) perception of the market (Kramer, 2004). Thus, the test may not be particularly helpful where the contracting parties supply two opposing perspectives on what constitutes 'business efficacy' in a given circumstance. For example, while a plaintiff may expect that fairly standard structures have been put in place for a particular transaction in order to satisfy the business efficacy test, the defendant may believe that the absent structures are part and parcel of its competitive pricing below market rates, and thus, ought to balance out the deficiencies in structures.

The business efficacy test which may ultimately evoke and impose benchmark standards mismatches with the more entrenched 1603 caveat emptor (buyer beware) doctrine, enunciated in *Chandelor v Lopus*. [5] The case predates Bowen LJ's business efficacy test and requires a (buyer) contracting party to carry out due diligence regarding the fitness and efficacy of whatever was offered. The obligation to beware and make business decisions based on the visible qualities of what a party is offering especially in commercial dealings is inarguably incompatible with Bowen's *ex post facto* test, and there was no illuminating commentary in *The Moorcock* vis-à-vis the intersection and overlap between the caveat emptor doctrine and business efficacy test. As Mustill LJ pointed out in a case,[6] the diametric views of contracting parties on what could satisfy the business efficacy test, leaves the judge to inevitably choose either of the parties' views or impose its own.[7]

Lastly, about half a century after the decision in *The Moorcock*, Lord Mackinnon developed the 'officious bystander' test in *Shirlaw v Southern Foundries (1926).* [8] The test is based on his proposition that "If, while the parties were making their bargain, an officious bystander were to suggest some express provision for it in their agreement, they would testily suppress him with a common 'Oh, of course!'".[9] Again, the officious bystander test runs counter to the caveat emptor doctrine because while the doctrine (especially in a sale contract) is rooted in the personal knowledge of a buyer-party to the contract, the officious bystander's interjection is made without personally being knowledgeable about the facts that birthed the disputed contract.

Apart from the two forgoing tests by Lords Bowen and Mackinnon, there have been considerable efforts in the 21st century by some UK apex judges in providing further and better clarity on the elusive formulae for ascertaining implied terms of facts. Such notable cases are Lord Hoffmann's *Belize Telecom* (2009), [10] and Lord Neuberger's *Marks & Spencer* (2015).[11] And more recently in 2023, the UKSC decision in *Barton v Morris.* [12] Although these cases have made important progress in creating methodologies and formulae for ascertaining what should constitute implied terms in

[1] *Chartbrook Ltd v Persimmon Homes Ltd* [2009] UKHL 38, para 25.

[2] See *Luxor (Eastbourne) Ltd v Cooper* [1941] AC 108, 120-121 (per Lewison LJ).

[3] *The Moorcock* (1889) 14 PD 64 (per Bowen LJ).

[4] Ibid, 68.

[5] *Chandelor v Lopus* (1603) 79 ER 3.

[6] *Torvald Klaveness A/S v Arni Maritime Corporation* [1994] 1 WLR 1465 (HL).

[7] Ibid, 1473.

[8] *Southern Foundries (1926) Ltd v Shirlaw* [1939] 2 KB 206 (CA).

[9] Ibid, 227.

[10] *Attorney General of Belize v Belize Telecom Ltd* [2009] UKPC 10. The facts and analysis are provided in part 4 below.

[11] *Marks and Spencer plc v BNP Paribas Securities Services Trust Company (Jersey) Ltd* [2015] UKSC 72. Hereinafer to be referred to as "Marks and Spencer". See part 5 below for the facts and analysis.

[12] Barton & Ors v Morris & Anor [2023] UKSC 3. See part 5 below for the facts and analysis.

contracts, this paper argues that the contemporary methodologies are yet to be sufficiently clear as evidenced by case law and scholarly opinions. Moreover, in Nigeria, the *Barton* decision arguably stands in opposition with Nigerian case law on contracts which formed around the traditional tests of implied terms, unjust enrichment and equitable maxims. Thus, *Belize Telecom, Marks and Spencer* and *Barton v Morris* have not been cited in any Nigerian case. The contents of Nigerian case law on implied terms are solely formed by the traditional tests: therefore, it is not yet clear how Nigerian courts would apply (or if they would be interested in applying) the ratios of these cases.

The central question which is herein investigated is therefore this: In what ways do the contemporary English case law on implied terms contradict with the established modes of making contracts as well as the doctrines of equity and unjust enrichment? This article would doctrinally unpack this central question throughout the six parts of this article, which includes this introduction. Part two discusses the article's scope, distinguishing agreements which require terms to be implied into them to give business efficacy and those called *agreement-to-agree* due to lack of fundamental terms to form valid contracts. Parts three and four discuss the law of implied terms from *The Moorcock* and *Shirlaw* purviews, up to the Privy Council decision in *Belize Telecom.* Here, the extent to which interpretation and implication of terms overlap are examined–this stems mainly from Lord Hoffmann's attempt to merge both concepts. In part five, the post-Belize UKSC cases—*Marks & Spencer* and *Barton v Morris*—are discussed, pointing out both the defects in the contemporary framework as well as the contradictions that ultimately fail to provide guidance to prospective contracting parties. The paper concludes in part 6 with recommendations and the way forward.

2. Scope of Discourse: Implied Terms of Fact Distinguished from Agreement-to-Agree and Terms Implied by Law

The article's discourse captures two possible types of incompleteness in contract-making for which a reasonable third party (courts) may be requested to enforce. For example, master agreements are by nature incomplete in factual terms due to their design for indefinite application. Where contracting parties deliberately execute an incomplete agreement for whatever reason, courts will usually assess whether such agreement as is, qualifies to be enforced after infusion of reasonable terms; or whether it is simply an agreement-to-agree due to lack of fundamental terms. If an incomplete contract's missing terms are not sufficiently fundamental, a court may under its inherent power to do justice, fill the gaps with reasonable terms that consequently bind the parties. This power of court derives from the presumption that contracting parties enter into agreements for the primary purpose of performance, and where they deliberately left out certain terms, the omission will not necessarily invalidate the contract. This differs from an agreement-to-agree where the missing terms are so fundamental that any attempt by a court to fill the gap invariably leads to a unilateral making of contract for the parties.

The consequential outcome of a judicial repair of agreement-to-agree philosophically runs contrary to the essence of contract as well as the function of courts as unbiased umpires in adversarial systems. What can thus be ascertained from the forgoing is that common law courts tend to have two polarized solutions for incomplete contracts. First, in assessing incompleteness, they ascertain whether the missing terms are too fundamental such that a repair will lead to making a brand new contract for the parties. If this is the case, common law courts will declare the contract to be an agreement-to-agree and thus unenforceable. Secondly, the court determines whether the missing terms are insufficiently fundamental in which case the missing terms can be filled with reasonable terms *suo moto*. In other words, in respect of incompleteness, courts will either enforce a contract after a minor repair, or not enforce it if repair is considerably fundamental.

In *Société Générale, London Branch v Greys*,[1] Lady Hale reiterated the two possible types of implied terms in contract. The first, with which this article is concerned, relates to a term being implied into a particular contract to give it a business efficacy in the light of the express terms, commercial common sense, and the facts known to both parties at the time the contract was made. In Nigeria, Justice Uwaifo in *Ibama v Shell*,[2] opined something similar that "there are

[1] [2012] UKSC 63, para 55.

[2] *Ibama v. Shell Pet. Dev. Co. (Nig.) Ltd (1998) 3 NWLR (Pt. 542) 493.*

certain contracts where terms may be logically implied from the express terms of the contract, or where no such express words are available, implied terms may be imported into the contract in so far as they do not contradict the express terms of the particular contract."[1]

The second type of implied terms arises by operation of law, and its validity does not depend necessarily on the presumed intention of the parties. This article does not discuss incompleteness in the context of agreement-to-agree, neither does it focus on terms implied by law. Terms to be implied by law are those terms that can be found in legislations and do apply across board for contracts that have the same subject matter irrespective of the parties' presumed intention. Thus, the article will unpack the implication of 'incompleteness' in contracts on ad hoc basis, i.e., based on certain facts or assumptions which may or may not exist in each and every circumstance. Incompleteness and gap-filling go hand in glove. Gap-filling is part of interpretation: thus, in interpreting a contract between two parties, the court usually identifies the presumed stronger party or drafter of the contract and leans in favor of the presumed weaker counterparty. If there is an ambiguity in drafting, courts would normally apply the *contra proferentem* rule to resolve the ambiguity or incompleteness against the drafter (McCunn, 2019).

Similarly, if the contract terms are unconscionable and unfair against a party, courts would likely presume the existence of arbitrariness and one-sided bargain which runs counter to the presumption of equality and fairness in contractual bargains. Until *Belize Telecom* in 2009, whichever of the above methods a court employed to supply implied terms ultimately satisfied the two leading tests of 'business efficacy' and 'officious bystander'. However, post-*Belize Telecom*, the jurisprudence of implied terms of fact has arguably oscillated to the realm of vagueness and opacity. In part three below, the two traditional tests and their contemporary relevance to the discourse will be discussed.

3. Historical Tracings of Implication of Terms in Fact: The Business Efficacy and Officious Bystander Tests

Ascertaining what is an express term of a contract as well as its meaning is arguably more straightforward compared to the implied terms of such a contract (Wilmot-Smith, 2023). Implied terms arise from the seeming necessity of incompleteness due to future exigencies; or unknowingly, from the imperfections of the language of contract. As stated earlier, there could be legitimate reasons for executing an incomplete contract and such reasons may be within the contemplation or intention of the parties; although in dispute, each of them may disagree on the terms that were commonly but indirectly thought to apply. Implied terms of a contract are as applicable as their express term counterparts: the main distinction is that implied terms are the invisible extensions of express terms. Notably, both express and implied terms are weighted equally in the eyes of the law, although in case of the latter, the challenge lies in its lack of immediate visibility and the necessity of being discovered as a precondition for application.

Prior to 1889, what existed what a random set of methods that litigants employed for ascertaining implied terms of fact. However, in *The Moorcock* case, Bowen LJ crafted the business efficacy test as guiding formula. Accordingly, a factual term can be implied into a contract based on the contracting parties' presumed intention, if such term gives business efficacy to the contract. Bowen's reasoning in *The Moorcock* is not surprising because during the late 19th century, English contract law was dominated by the activities of merchants. English contract law's mercantile origin is hardly in contention and has been acknowledged by many English scholars. Lord Devlin (1951), in this extrajudicial piece, explained this mercantile heritage and why contractual interpretation especially in commercial dealings cannot reasonably disentangle from the (evolved) *lex mercatoria* and customs of English merchants (Steyn, 1997; Mitchell, 2003).

Based on the forgoing perception, it is unsurprising that the facts which gave birth to the business efficacy test in *The Moorcock* were commercial in nature, involving a maritime shipping contract. In the case, a cargo ship was damaged during the time it was docking at the defendant's jetty in River Thames, England. The cause of damage on the vessel was ascertained to have resulted from the jetty's insufficient fitness for purpose, the vessel having been

[1] Ibid, 496.

damaged by a ridge of hard ground on the riverbed. Bowen LJ, held the defendant liable for breach of an implied term to keep the river bed reasonably fit for purpose, a conclusion he believed could not have differed from the presumable expectation of the parties about the safety level of the jetty in ensuring that steamships load and offload cargoes safely.

Accordingly, both parties were in the business of maritime shipping and it was therefore reasonably expected that a term ensuring against the damage of the plaintiff's vessel would be implied into the contract to provide such business efficacy. In the words of Bowen LJ, "[t]he law is raising an implication from the presumed intention of the parties with the object of giving to the transaction such efficacy as both parties must have intended that at all events it should have. In business transactions such as this, what the law desires to effect by the implication is to give such business efficacy to the transaction as must have been intended at all events by both parties."[1]

A self-evident challenge with the business efficacy test lies in the specialized nature of knowledge and experience needed to exactly ascertain it in a given circumstance. Its ascertainment by courts tends to be largely derived from the parties' presumed intention as experienced businessmen. Alternatively, where the parties are diametrically opposed as to what constitutes business efficacy in a circumstance, the court would have to rely on a third party expert opinion. Lord Bowen's test in the 19th century continued to influence legal scholars and judges in their approach towards contract interpretation.

In fact, much of the solution crafted by English judges in the 20th century in respect of interpretation of commercial contracts revolved around the commercial sense approach (Andrews, 2017). Lord Wilberforce[2] and Lord Diplock[3] were among the English judges whose interpretive solutions anchored largely on business common sense. In any case, the sophisticated nature of the business efficacy test evoked much uncertainty around its determination and application. There were also cost implications especially where the parties are in disagreement on what is commercially efficacious. This necessitated the need for a simpler test for denoting implied terms, perhaps to be rooted in common sense (Kramer, 2003), instead of in business efficacy.

The second test, the officious bystander test is based on a legal fiction and was somewhat a departure from the business sense approach. Its foundational notion anchors on the sensibilities of a random reasonable person portrayed to possess an omniscient ability. Presumably, the law would make do with what such a person eavesdropping on contracting parties' conversations about their contract terms would hastily think to be an express term of that contract. Before the official birth of the officious bystander test, forerunner efforts were already undertaken by Lord Scrutton: the foundational elements of the test were developed in *Reigate v. Union Manufacturing Company,*[4] in which mutual trust and confidence as well as their practical effects were implied into an employment contract. According to Scrutton, "[a] term can only be implied if it is necessary in the business sense to give efficacy to the contract".[5] He added that a term would only be implied if "it is such a term that it can confidently be said that if at the time the contract was being negotiated the parties had been asked what would happen in a certain event, they would both have replied 'Of course, so and so will happen; we did not trouble to say that; it is too clear'".[6]

Two decades after *Reigate*, MacKinnon L.J. in *Shirlaw* v. *Southern Foundries (1926) Limited,*[7] crafted the 'officious bystander' test. The officious bystander test arguably requires a lower threshold of proof compared to the business efficacy test because according to Mackinnon, the term to be implied has to be so apparently obvious such that if such term had been suggested for inclusion by an officious bystander when the parties were making the contract, they would without hesitation say 'of course!'[8]

Following the *Shirlaw* case, the difficulty that courts encountered in applying the officious bystander test related to the threshold of

[1] *The Moorcock* (1889) 14 PD 64 (CA) 68, Bowen LJ.

[2] See *Prenn v Simmonds* [1971] 1 WLR 1381, 1389 HL ("commercial good sense").

[3] See *Antaios Cia Naviera S.A. v Salen Rederierna AB* [1985] AC 191, 201 HL ("business common sense").

[4] [1918] 1 KB 592.

[5] Ibid, 605.

[6] Ibid.

[7] [1939] 2 KB 206 (CA).

[8] Ibid, 227.

knowledge and commercial awareness a person must possess in order to qualify for the role of being consulted by the parties. It gradually became obvious that while the test may be useful in apparently obvious cases with simple facts, in circumstances where the parties are dealing with complicated sets of facts within a specialized commercial area, the officious bystander test became insufficient to accurately ascertain implied terms.

The forgoing view accords with Lord Neuberger's in *Marks & Spencer* when he opined that "[t]he notion that a term will be implied if a reasonable reader of the contract, knowing all its provisions and the surrounding circumstances, would understand it to be implied is quite acceptable, provided that (i) the reasonable reader is treated as reading the contract at the time it was made and (ii) he would consider the term to be so obvious as to go without saying or to be necessary for business efficacy. (The difference between what the reasonable reader would understand and what the parties, acting reasonably, would agree, appears to me to be a notional distinction without a practical difference.)." [1] The consensus among 21st century judges, championed by Lord Hoffmann in *Belize Telecom*, seems to be that elements of the traditional tests be used as tools, jointly and severally, when faced with the task of ascertaining implied terms.[2]

Legal historians would recall the staggered growth of the common law over several centuries (Baker, 2019). Its hardening process as a coherent body law took centuries to crystallize, and the foundational principle of *stare decisis* requires that common law judges treat similar cases alike (Cross & Harris, 1991). However, as society evolves, facts of disputes would naturally deviate from previously recognizable patterns, and viable solutions would consequently be adjusted or completely overhauled. As exemplified by the 1889 *Riggs v Palmer*, [3] the ensuing complexities of legal evolution require judges under the mandate of *ibi jus ibi remedium* to be disruptively inventive in providing remedies for hard cases (Dworkin, 1977). The forgoing tests for ascertaining implied terms had come during the era of rapid legal evolution, and it was frustrating to frequently encounter situations in which the available tests or remedies were insufficient to deal with a present situation. As the evolution of law could not keep pace with the fast evolving commerce, the potency of common law rules vis-à-vis commercial dealings were constantly challenged and judges craved for malleable tools that could fit in most situations.

Consequently, the rise of reasonableness/reasonable man's perspective as a tool of interpretation became increasingly mainstream. As was confirmed by Lord Wright (1935), reasonableness (the contemporary equivalent of public policy), also became a judge's leeway to infuse their own educated intuitions and conscience in solving legal problems. Lord Denning (a chronic dissenter) was in the vanguard of this approach as he demonstrated in many cases including his opinion at the Court of Appeal in *Liverpool City Council* v. *Irwin*.[4] In that case, the tenants of the Liverpool City Council withheld payment of rents in protest and the Council sought to evict them.

The tenants' leading issue was whether there was a contract and if so whether an implied term requiring the Council to properly maintain the common areas could be added. The tenants argued that the duty to maintain the common areas of the building was an implied term for which the Council failed to uphold. The House of Lords in *Irvin*,[5] agreed that there was an implied term that required the Council to take reasonable care in maintaining the common areas because such maintenance was necessary for the tenancy to function properly. As Lord Wilberforce emphasized, "such obligation should be read into the contract as the nature of the contract itself implicitly requires, no more, no less: a test, in other words, of necessity."[6]

At the Court of Appeal stage of the *Irvin* case, Lord Denning M.R had slightly dissented, opining that the test for implying a term, based upon the presumed intention of the parties, was "whether or not it was *reasonable in all the circumstances* to do so."[7] As glowingly evident in his book titled the *Discipline of Law* (1979), Denning often abandoned the strict constructionist approach to law, and was a

[1] See *Marks and Spencer* [2015] UKSC 72, para 23.

[2] The *Belize Telecom* case (2009) para 21.

[3] 115 NY 506 (1889).

[4] [1976] QB 319.

[5] [1977] AC 239, HL.

[6] Ibid, pp 254F-255A.

[7] [1976] QB 319, 330.

purveyor for deepening the role of reasonableness as well as what he described in *Dennis Reed Ltd* as "the common understanding of men".[1] He often used the term "man on the Clapham omnibus" as a measurement standard for what could pass muster in legal reasoning (Jewel, 2019). Admittedly, the Clapham omnibus term predates Denning, having been enunciated in 1903 in *McQuire v. Western Morning News Co*,[2] and appeared later in a number of non-contract cases such as *Hall v. Brooklands Auto-Racing Club*.[3] In any event, Denning used the term in a number of cases including in *Miller v. Jackson*,[4] to emphasize reasonableness, fairness, and public policy as tools of interpretation as well as a formula for ascertaining what term could be implied into a contract.

We would recall that at common law, the terms of contracts enjoy a bifurcated division into express and implied terms. The first is somewhat easier to prove because express terms either exist textually, or orally and by conduct. In *Carmichael v National Power Plc*, [5] Lord Hoffmann (with whom two other justices agreed) recognized the equality of these three modes of making contracts at common law. In that case the parties had intended that their contract be partly contained in letters, oral exchanges at the job interviews or elsewhere, and partly left to change via conduct as time proceeded. The court held that where the objective intention of contracting parties requires being gathered partly from documents as well as from oral exchanges and conduct, the terms of the contract are a question of fact which can be gleaned from any of such modes of contract-making. In other words, implied terms of fact are simply unexpressed intentions that have to be elicited by a reasonable inference to understand what the contract means. Thus, both express and implied terms enjoy equality in contractual interpretation. This accords with Lord Hoffmann's view that "[t]he implication of the term is not an addition to the instrument. It only spells out what the instrument means."[6]

However, based on the hindsight knowledge of case law, common law judges have struggled over the task of ascertaining implied terms without falling into the fundamental error of making new contracts for parties. This is because unlike express terms that clearly harbor the intention of parties, ascertaining actual implied terms comes from a general experience in that contractual subject matter. This is where the business efficacy and officious bystander tests come in—conclusively, the business to be made efficacious must relate to that which forms the subject matter of contract, and the officious bystander eavesdropping at keyholes to the parties' conversation must at least be fairly knowledgeable and experienced in the contract's subject matter to be able to make any reasonable interjections.

The forgoing however is somewhat different from Lord Denning's approach, which emphasized the perspective of the man on Clapham omnibus—Denning's approach is a much laxer method which presumes that a regular/random individual on a public bus could be sufficiently knowledgeable as to arbitrate or proffer reliable opinions that will not only be able to resolve a difficult contractual issue but also act as a final arbiter in the commercial parties' opposing views (Moran, 2003). Arguably, in this modern time, use of Denning's approach should be discouraged in interpreting or ascertaining implied terms of contracts, especially in complex/niche business areas. But as would be shown below in part 4, judges after the era of Denning have not performed spectacularly well in easing the confusion that surrounds implied terms. In fact, they have arguably intensified it—Lord Hoffmann's decisions (to be discussed below) have stirred roughly the somewhat settled methods that were based on the business efficacy and officious bystander tests.

4. Lord Hoffmann: The Overlap Between Implication of Terms in Fact and Contract Interpretation

4.1 Lord Hoffmann Before the Belize Telecom Case

Before Lord Hoffmann's decision in *Belize Telecom*, he had already acquired a reputation in contract interpretation which emphasized the infusion of background facts in realizing the presumed intention of the parties (Tan, 2016). This contextualist approach sits uneasily in contrast with the formalistic approach to interpretation which has been integral in the reputation of English contract as predictable,

[1] *Dennis Reed Ltd v Goody* [1950] 2 KB 277, 284.

[2] [1903] 2 KB 100, CA.

[3] [1932] 1 KB 205.

[4] [1977] QB 966.

[5] [1999] 1 WLR 2042, 2049.

[6] See the *Belize Telecom* case (2009), para 18.

whose judges typically vote for predictable justice in commerce even if the heavens were to fall (Charny, 1999; Wilkinson-Ryan, 2015; Jonathan, 2013). Scholarly commentaries have suggested that such level of predictability was commercially efficient for England especially in relation to its mission to be a jurisdiction of choice for international commercial dispute settlement (Atiyah & Summers, 1987; McKendrick, 1997).

However, in many ways, the 21st century Hoffmann may be comparable to his 20th century Denning predecessor who utilized every opportunity—for example—the *High Trees* case,[1] to jettison formalism in preference for context, equity and justice. For Hoffmann, the devil is in the detail: thus, during his active days in the House of Lords, he often considered the prevalent rules of contract interpretation too formalistic to provide true justice to contracting parties, and his key decisions sought frantically for the truth in contexts at the expense of formalism and predictability. Notably, Hoffmann's decision in *ICS v West Bromwich*[2] was designed (perhaps unintentionally) to rock a somewhat stable boat that sailed on formalism with the overall perception that the dangers of formalism often surpassed its advantage of predictability.

Thus, Hoffmann's opinion in *Belize Telecom* in relation to implied terms was already expressed a decade earlier in his five principles of contractual interpretation in *ICS*, particularly the fourth principle which states that "the meaning of a document may not be the same as the meaning of the words used. The court can and should attempt to ascertain what the words were intended to convey as opposed to their literal meaning."[3] Similarly, in the first of the five principles, he admonishes courts "[t]o consider the meaning a document would convey to a reasonable person having all the background knowledge that would reasonably have been available to the parties at the time the document was made."[4]

Hoffmann's criterion of a reasonable person including their use as a yardstick for appreciating gaps in contract is undoubtedly higher than Denning's, because it is rooted in the reasonable person's ability to first of all acquire all the necessary background knowledge and information that would reasonably have been available to the parties at the time the document was made. This is different from Denning's approach which only emphasized reasonableness based on the perception of a man on the Clapham omnibus. Nigerian courts tend to now share the view that more than reasonableness is required as a yardstick for contract interpretation and in ascertaining implied terms. In *Okoebor v. Eyobo Eng. Serv. Ltd*,[5] the Court of Appeal held that "parties ought not to imply a term merely because it would be a reasonable term to include in a contract. It must be such a necessary term that both parties must have interpled that it should form part of the contract and have only not expressed it because its necessity was so obvious that it was taken for granted."[6]

Returning to Hoffmann, it may be fair to argue that during his time, the English rules of contractual interpretation, as well as the methods in vogue for ascertaining implied terms, were perceptively unstable and incapable of providing just outcomes. Part of that perception stemmed from the rigidity and harshness of the Parol evidence rule (triggered by the inclusion of an *entire agreement* clause) which naturally excluded the possible admissibility of relevant background facts that could assist in ascertaining the contracting parties' true intention (Posner, 1998; Linzer, 2002; Zuppi, 2007). Thus, apart from the ratio in the *ICS* case which emphasized the necessity of going beyond the four walls of the contract into its relevant background facts, Hoffmann further developed this view in *Chartbrook Ltd v Persimmon Homes Ltd*.[7] In *Chartbrook*, Hoffmann's previous obsession with infusing background facts into contract had hardened into the radical point of proposing that judges unilaterally amend contracts "[i]f they believe that something has gone wrong with the language of the contract … they may proceed with a red ink to verbally rearrange and correct

[1] *Central London Property Trust Ltd v* High Trees *House Ltd* [1947] KB 130. Before *High Trees*, a promise made without a consideration was clearly unenforceable. Denning however created the doctrine of promissory estoppel to prevent a party from reneging on their promise if the counterparty has reasonably relied on that promise.

[2] [1998] 1 WLR 896.

[3] Ibid, 912-13.

[4] Ibid.

[5] (1991) 4 NWLR (Pt. 187) 553.

[6] Ibid, 555.

[7] [2009] UKHL 38.

provisions of the contract without any limitation."[1] As would be shown below in the facts and holding of *Belize Telecom*, Hoffmann approach increasingly blurred the line between interpretation and implication.

4.2 AG of Belize v Belize Telecom Ltd: Lord Hoffmann Attempts to Merge Implication and Interpretation

The facts of *Belize Telecom*[2] are as follows: the government of Belize decided to privatize the nation's telecommunication services. The Articles of Association of Belize Telecommunications Ltd provided for special class 'C' shares. Accordingly, "the holder of the Special Share shall so long as it is the holder of 'C' Ordinary shares amounting to 37.5% or more of the issued share capital of the Company be entitled at any time by written notice served upon the Company to appoint two of the Directors designated 'C' Directors and by like notice to remove any Director so appointed and appoint another in his or her place."[3]

Self-evidently, the Company's Articles of Association were, however, silent on how a shareholding below 37.5% would impact on the holder's power to appoint or remove directors. Belize Telecom Ltd, holding the requisite number of shares was able to appoint two directors. However, within a year of appointment, owing to financial difficulties, its shareholding in the class 'C' shares fell below 37.5%. Given that the Articles of Association were silent on how the directors appointed by the holder of the special share would be removed when the latter's shareholding had fallen below 37.5%, a dispute consequently arose.

Belize Telecom Ltd argued that owing to the silence on how the directors would be removed if Belize Telecom's shareholding fell below the minimum percentage, the directors were consequently "irremovable" unless they choose to resign voluntarily.[4] Similarly, Belize Telecom Ltd argued that the court lacked the power to introduce new terms into the written document (Articles of Association) because that would amount to rewriting the contract for the parties. The Attorney General of Belize argued otherwise, emphasizing the 'absurdity' of a situation in which the directors would become irremovable due to the lack of an expressly stated condition. Thus, in the absence of such an express term about their removal when the majority shareholding falls below the minimum percentage, the court ought to imply the term of the directors' resignation into the contract (Articles of Association).[5]

The Privy Council reversed the decision of the Court of Appeal of Belize, holding that the directors' resignation and vacation of office could be implied into the contract in the absence of any shareholder in possession of the minimum of 37.5% to appoint or remove them. The Privy Council opined that the implied term was "required to avoid defeating what appears to have been the overriding purpose of the machinery of appointment and removal of directors, namely to ensure that the board reflects the appropriate shareholder interests in accordance with the scheme laid out in the articles".[6]

The Privy Council's decision was unanimous. Although it was delivered by Lord Hoffmann, Lords Rodger, Carswell, Brown, and Baroness Hale, agreed with Hoffmann. Yet, anyone who is familiar with Lord Hoffmann's works would recognize the *Belize Telecom* decision as his brainchild because the *Belize* principles as outlined below are largely consistent with his views in the *ICS* and *The Achilleas*,[7] cases. Shortly after the *Belize* judgment in 2009, Lord Clarke MR predicted that Lord Hoffmann's analysis "will soon be as much referred to as his approach to the construction of contracts in Investors Compensation Scheme [1998] 1 WLR 896, 912-913".[8] The principles enunciated in *Belize* can be gleaned from the following quotes of the case and their resemblance with the *ICS* restatement is equally noted. In the case, Hoffmann noted that:

1) The court has no power to improve upon the instrument which it is called upon to construe, whether it be a contract, a statute or articles of association. It cannot introduce terms to make it fairer or more

[1] Ibid, para 25. Also see para 14 thereof.

[2] *Attorney General of Belize v Belize Telecom Ltd* [2009] UKPC 10. Hereafter referred to as: *Belize Telecom* or *Belize.*

[3] The *Belize Telecom* case, para 5.

[4] Ibid, para 14.

[5] Ibid.

[6] Ibid, para 32.

[7] *Transfield Shipping Inc v Mercator Shipping Inc* (The Achilleas) [2008] UKHL 48, paras 25 and 26.

[8] *Mediterranean Salvage & Towage Ltd v Seamar Trading & Commerce Inc* [2009] EWCA Civ 531, para 8.

reasonable. It is concerned only to discover what the instrument means. However, that meaning is not necessarily or always what the authors or parties to the document would have intended. It is the meaning which the instrument would convey to a reasonable person having all the background knowledge which would reasonably be available to the audience to whom the instrument is addressed.[1]

2) The question of implication arises when the instrument does not expressly provide for what is to happen when some event occurs. The most usual inference in such a case is that nothing is to happen. If the parties had intended something to happen, the instrument would have said so. Otherwise, the express provisions of the instrument are to continue to operate undisturbed. If the event has caused loss to one or other of the parties, the loss lies where it falls.[2]

3) In some cases, however, the reasonable addressee would understand the instrument to mean something else. He would consider that the only meaning consistent with the other provisions of the instrument, read against the relevant background, is that something is to happen. The event in question is to affect the rights of the parties. The instrument may not have expressly said so, but this is what it must mean. In such a case, it is said that the court implies a term as to what will happen if the event in question occurs. But the implication of the term is not an addition to the instrument. It only spells out what the instrument means.[3]

4) The proposition that the implication of a term is an exercise in the construction of the instrument as a whole is not only a matter of logic (since a court has no power to alter what the instrument means) but also well supported by authority.[4]

5) It follows that in every case in which it is said that some provision ought to be implied in an instrument, the question for the court is whether such a provision would spell out in express words what the instrument, read against the relevant background, would reasonably be understood to mean. It will be noticed from Lord Pearson's speech that this question can be reformulated in various ways which a court may find helpful in providing an answer—the implied term must "go without saying", it must be "necessary to give business efficacy to the contract" and so on—but these are not in the Board's opinion to be treated as different or additional tests. There is only one question: is that what the instrument, read as a whole against the relevant background, would reasonably be understood to mean?[5]

As earlier stated, there is a noticeable pattern of radicalism in Lord Hoffmann's approaches to legal reasoning in contracts which tended to always reinvent the wheel. First, in his *ICS* case, he stated boldly that his five restatement "had discarded almost all the old intellectual baggage of interpretation."[6] Thus, in terms of formula, he hoped that the five restatements in *ICS* would be taken as the primary guide for contract interpretation, even though, arguably, the decision's roots in contextualism did not provide a clearly objective formula for this purpose. As could be seen from the later reactions of his peers, such as Lord Neuberger[7] and Lord Hodge,[8] the *ICS* (and *Chartbrook*) reasoning did not enjoy the unopposed sacrosanct position its creator had envisioned.

Secondly, in the Privy Council case of *BP Refinery (Westernport) Pty Ltd v President, Councillors and Ratepayers of the Shire of Hastings*,[9] Lord Simon (speaking for the majority, which included Viscount Dilhorne and Lord Keith) said that "[F]or a term to be implied, the following conditions (which may overlap) must be satisfied: (1) it must be reasonable and equitable; (2) it must be necessary to give business efficacy to the contract, so that no term will be implied if the contract is effective without it; (3) it must be so obvious that 'it goes without saying'; (4) it must be capable of clear expression; (5) it must not contradict any express term of the contract."[10] However, in the

[1] The *Belize Telecom* case, para 16.

[2] Ibid, para 17.

[3] Ibid, para 18.

[4] Ibid, para 19.

[5] Ibid, para 21.

[6] *ICS v West Bromwich* [1998] 1 WLR 896, 912.

[7] *Arnold v Britton* [2015] UKSC 36, paras 17-21.

[8] Ibid, para 66 (Lord Hodge agreed with Lord Neuberger).

[9] (1977) 52 Australian Law Journal Report 20.

[10] Ibid, 26.

Belize case, Hoffmann arguably watered down the application of over a century's set of tests in determining implied terms of fact when he opined that the tests assembled by Lord Simon were not independent tests per se, but "a collection of different ways in which judges have tried to express the central idea that the proposed implied term must spell out what the contract actually means, or in which they have explained why they did not think that it did so."[1]

Similarly, Hoffmann's attempt in *Belize Telecom* to merge implication of terms in contract with contractual interpretation was not a product of necessity born out of the facts of *Belize*. Arguably, the outcome was based on a premeditated approach to expand his *ICS* legacy, considering his attempts to merge both concepts in at least two occasions that spanned over a decade. Hoffmann (1995, p. 139), argued in this extrajudicial piece published in The Law Teacher, that "[t]he officious bystander test diverts attention from the fact that the implication of terms into a contract is in essence a question of construction like any other". Two years later in *South Australia Asset Management Corporation v York Montague Ltd.*,[2] he similarly opined that "[a]s in the case of any implied term, the process is one of construction of the agreement as a whole in its commercial setting".[3] The *Belize* decision was therefore a continuation of his mission to considerably blur the line of difference between the two legal concepts, which ultimately deepened the confusion that already existed in this area of law.

However, Sir Thomas Bingham elucidated in *Philips Electronique Grand Public SA v British Sky Broadcasting Ltd*,[4] regarding the core difference between both concepts when he opined that "the courts' usual role in contractual interpretation is, by resolving ambiguities or reconciling apparent inconsistencies, to attribute the true meaning to the language in which the parties themselves have expressed their contract. The implication of contract terms involves a different and altogether more ambitious undertaking: the interpolation of terms to deal with matters for which, ex hypothesi, the parties themselves have made no provision. It is because the implication of terms is so potentially intrusive that the law imposes strict constraints on the exercise of this extraordinary power."[5] Six years after *Belize Telecom*, Lord Neuberger's lead opinion in *Marks & Spencer* further clarified the lingering confusion on the role of the traditional tests vis-à-vis Hoffmann's *Belize* in ascertaining implication of terms in fact.

5. Implication of Facts in Contracts After *Belize Telecom*

5.1 Marks and Spencer plc v BNP Paribas[6]*: Necessity Trumps over Reasonableness*

Marks and Spencer plc (M&S) was a tenant under a commercial lease with BNP Paribas as the landlord. M&S exercised its right under the agreement's break clause to determine the lease on 24 January 2012, earlier than 2 February 2018, when the lease was scheduled to naturally expire. Although the rent was payable in advance on the usual quarter days, M&S had already paid rent in advance for the entire quarter due on 25 December 2011. The issue was whether it can recover from the landlords the apportioned rent in respect of the period from 24 January to 24 March 2012.

The lease did not expressly state that the landlord was required to refund any overpaid rent. M&S argued that a term should be implied into the lease requiring BNP Paribas to refund the overpayment. Given the absence of a provision in the Lease which expressly obliges the landlords to pay the apportioned sum to the tenant. Accordingly, the court held that in order to succeed the claimant has to establish that such an obligation must be implied into the lease. Lord Neuberger read the lead judgment (with Lord Carnwath slightly dissenting). Here, it is important to note that Neuberger has been a fierce opponent of Hoffmann, disagreeing with him in a number of cases, especially on his *ICS and Chartbrook* judgments, on the most appropriate method for contract interpretation. While Hoffmann is a proponent of contextualism, Neuberger has insisted that a literal interpretation rooted in the Parol evidence rule offers more predictability to contracting parties and prevents the court from shielding an "unwise" party from their decisions and

[1] The *Belize Telecom* case, para 27.

[2] [1997] AC 191.

[3] Ibid, 212.

[4] *Philips Electronique Grand Public SA v British Sky Broadcasting Ltd* [1995] Entertainment and Media Law Report 472.

[5] Ibid, 481.

[6] [2015] UKSC 72. Hereinafter referred to as *Marks and Spencer*.

consequently rewriting contracts for parties.[1] Thus, for the sake of fairness, Neuberger's critique of Hoffmann's *Belize Telecom* should be appreciated alongside their intellectual disagreements.

In *Marks and Spencer*, Neuberger opined that a term will only be implied if it satisfies the test of business necessity. Apparently, in place of Bowen LJ's 'efficacy', he used the substitute of 'necessity' "[t]o emphasize that there has been no dilution of the requirements which have to be satisfied before a term will be implied, because it is apparent that Belize Telecom has been interpreted by both academic lawyers and judges as having changed the law."[2] He opined that "that both (i) construing the words which the parties have used in their contract and (ii) implying terms into the contract, involve determining the scope and meaning of the contract. However, Lord Hoffmann's analysis in Belize Telecom could obscure the fact that construing the words used and implying additional words are different processes governed by different rules. Of course, it is fair to say that the factors to be taken into account on an issue of construction, namely the words used in the contract, the surrounding circumstances known to both parties at the time of the contract, commercial common sense, and the reasonable reader or reasonable parties, are also taken into account on an issue of implication."[3]

Neuberger added that the forgoing "does not mean that the exercise of implication should be properly classified as part of the exercise of interpretation, let alone that it should be carried out at the same time as interpretation. When one is implying a term or a phrase, one is not construing words, as the words to be implied are ex hypothesi not there to be construed; and to speak of construing the contract as a whole, including the implied terms, is not helpful, not least because it begs the question as to what construction actually means in this context."[4] Similarly, "in most, possibly all, disputes about whether a term should be implied into a contract, it is only after the process of construing the express words is complete that the issue of an implied term falls to be considered. Until one has decided what the parties have expressly agreed, it is difficult to see how one can set about deciding whether a term should be implied and if so what term."[5] In what follows, the article will discuss *Barton* and its interface with the contract doctrine of unjust enrichment and quantum meruit.

5.2 Barton v Morris: A Shift Towards Unjust Enrichment and Quantum Meruit

In *Barton v Morris*,[6] an oral agreement was made between Mr. Barton and Foxpace Ltd ("Foxpace") — the latter owned a property (Nash House) which it wanted to sell. The express term based on the parties' oral agreement was that if Mr. Barton introduced to Foxpace a purchaser who bought Nash House for £6.5 million or more, Foxpace would pay Mr. Barton GBP1.2 million. Based on this term, Mr. Barton introduced Western UK Acton Ltd ("Western") to Foxpace to purchase the property for GBP6.55 million. However, upon discovery by Western that Nash House was located in a place awaiting to be constructed a rail link, the price was consequently impacted: it was eventually purchased for GBP6 million plus VAT.

The parties' oral contract was silent on what would happen in terms of Mr. Barton's remuneration if the property were to be sold less than GBP6.5 million. Foxpace argued that owing to the sale below GBP6.5 million it was relieved (based on the express term) from any obligation of paying the fee of GBP1.2 million or any amount whatsoever to Mr. Barton. The trial court agreed with this argument. The Court of Appeal disagreed and held for Mr. Barton, stating that he was entitled to a reasonable remuneration for his services. However, the Supreme Court disagreed and found favor in the trial judge's reasoning.

The central issue in *Barton* revolved around unjust enrichment and quantum meruit. First, Mr Barton was not a professional estate agent and in two occasions he had tried to purchase the Nash House and paid initial deposits altogether amounting to GBP1.2 million, but for various reasons he could not finalize the purchase. Consequently, these deposits to Foxpace were forfeited. Based on the forgoing, Mr. Barton agreed provide a buyer who will purchase the Nash House for GBP 6.5 million or

[1] *Arnold v Britton & Ors* [2015] UKSC 36, para 20.

[2] *Marks and Spencer*, para 24.

[3] Ibid, para 26.

[4] Ibid, para 27.

[5] Ibid, para 28.

[6] [2023] UKSC 3. Hereinafter referred to as *Barton* or *Barton v Morris*.

higher in exchange of recovering the forfeited GBP1.2 million. The issue for determination can thus be surmised as follows: where contracting parties agree orally that an introduction fee (GBP1.2 million) would be paid upon a property being sold for a particular amount (GBP6.5 million), and the property eventually sold for £6 million, less than that conditional amount of GBP6.5 million, does the seller have an obligation, whether contractual or non-contractual, to pay reasonable remuneration to the introducer for their services?

The UKSC by a 3-2 majority, held that implying a term requiring payment to Mr. Barton, despite the sale price being below GBP6.5 million, was not necessary to give the contract business efficacy. For the Court, the express terms of the agreement were clear, i.e., payment of the GBP1.2 fee to Mr Barton was conditional upon achieving a sale price of GBP6.5 million or more. Thus, implying a term for payment under different circumstances would contradict the express terms of the agreement. The Court opined that the existence of a valid contractual agreement between the parties which embodies an express term precluded a claim for unjust enrichment based on the forfeiture. Similarly, the Court reasoned that since the parties had allocated the risk within their agreement, the Court was no longer in the position to reallocate that risk based on the outcome.

The *Barton* case rests largely on the earlier ratio in *Marks & Spencer* in which the doctrine of absolute necessity was instituted as a guide in determining whether a term should be implied into the contract of parties. Thus, if the need for implied terms is not absolutely necessary to reflect the parties' intentions and to make the contract workable, the court would refrain from providing implied terms. Although *Barton* is barely two years old, its rule is foreseen to be fiercely controversial because in adhering to the absolute necessity rule in *Marks & Spencer*, it denied the century old rule on unjust enrichment and quantum meruit. This is likely to generate more hardship in long term contractual transactions where performance has been substantially performed even though some aspects of the performance may not entirely sit with the initially agreed express terms—it should be taken to go without saying that the reasonable costs incurred by Mr. Barton deserved a reasonable recompense or that the forfeited sum of GBP1.2 million as well as the GBP 6 million sale both stemming from Mr. Barton's efforts deserve remuneration.

It is curious that the Court seemed to have abandoned the relevant maxims of equity, particularly the maxim that equity inputs an intention to fulfill an obligation where a substantial performance of an obligation is generally treated as sufficient.[1] Similarly, equity abhors a forfeiture.[2] Foxpace made a total sum of GBP 7.2 million pounds, i.e., at about GBP 700,000 above the proposed sale price of GBP6.5 million for which Mr. Barton would be paid. At least, a court of equity with good conscience should have awarded Mr. Barton the surplus of GBP700,000 as a reasonable remuneration to offset his already forfeited sum of GPB1.2 million as well as the personal expenses he incurred in connecting Foxpace with buyer—after all, "equity delights to do justice and not by halves"[3] to ensure that where a common law remedy is insufficient to render justice, equity will intervene.

In Nigeria, the facts of *Barton* would likely yield a different outcome: the Nigerian courts are likely to view Foxpace's acceptance of the GBP6 million purchase price (instead of GBP6.5 million) as modifying the earlier oral contract by conduct as well as creating a reliance-based estoppel on Foxpace not to revert to the original express term.[4] Mr. Barton would likely have been awarded a reasonable fee (perhaps the difference between Foxpace's minimum expectation of GBP6.5 million and the total of GBP7.2 million which it received) to offset his own expenses. Similarly, the forfeited GBP1.2 million would have been viewed as an unjust enrichment in light of Mr. Barton's efforts which

[1] See *Dakin & Co Ltd v Lee* [1916] 1 KB 566; *Hoenig v Isaacs* [1952] 2 All ER 176. In both cases the courts held that if a party has *substantially performed* a contract but with minor defects, they can still enforce the contract, subject to deductions for any deficiencies.

[2] See *Stickney v Keeble* [1915] AC 386, HL; *Shiloh Spinners Ltd v Harding* [1973] AC 691, HL; *Patel v Ali* [1984] Ch 283. These English apex cases affirm that equity would intervene to mitigate harsh legal consequences where strict forfeiture would be unfair, particularly when the defaulting party has made reasonable efforts to comply with obligations.

[3] See *Walsh v Lonsdale* (1882) 21 Ch D 9; *Beswick v Beswick* [1968] AC 58, HL; *Chappell v Times Newspapers Ltd* [1975] 1 WLR 482.

[4] See generally *Central London Property Trust Ltd v High Trees House Ltd* [1947] KB 130, Lord Denning (promissory estoppel).

led to more than 90% of the agreed sale price.[1] It is a trite principle that legal formalities should not to be weaponized to undermine genuine equitable interests. In other words, equity will not allow a statute or formality to be used as a cloak for injustice given its habit to prioritize substance over form.[2]

In light of these, Nigerian courts would likely arrive at an opposite result because in *Daspan v Mangu Local Govt Council*,[3] a case with related facts, the Nigerian Court of Appeal held that "an implied contract is one that is inferred from the conduct of the parties and which arises where a party without being requested to do so, renders services under circumstances indicating that he expects to be paid and the other party knowing such circumstances avails himself of the benefit of those services. In the instant case, the respondent had availed himself of the services of the architectural/mechanical drawings and made no move to stop the appellant from producing them." [4] In matters of justice, Nigerian (common law) courts would typically recall that *ubi jus ibi remedium*—equity will not allow a wrong to be suffered without a remedy.[5]

6. Recommendation and Conclusion

The practice of ascertaining implied terms has clearly been dominated by the inquisitorial system approach in which the judge could descend onto the arena of dispute without minding if their descent would be perceived as being a biased umpire. The early proponents of the current formula for ascertaining implied terms seemed to be English judges that leaned towards the inquisitorial systemic thoughts —for example— Lord Denning's legal reasoning in many of his judgments gave birth to several equitable principles, which ultimately resembled the byproducts of the inquisitorial system. But the common law system is adversarial in nature, and the question is what will an adversarial system, strictly speaking, do in relation to implied terms of fact where concepts like reasonableness, officious bystander, business efficacy are to be used to determine implied terms.

Admittedly, living up to the standards of the adversarial system where the judge is not purportedly the man on the Clapham omnibus will be costlier for litigants because of the obligation to use third party experts to determine the reasonableness and officious bystander views in a given circumstance. However, commercial parties may be willing to pay extra as part of court fees if involvement of a third party expert would produce better clarity and accuracy in the determinations of implied terms in complex commercial contracts; compared to the perceptions of judges who usually lack actual commercial experience.

The *Belize Telecom* decision rocked the stable boat of implied terms of fact by attempting to merge implication and interpretation outside the traditional tests of business efficacy and officious bystander. Lord Hoffmann's influence in Belize vis-à-vis the merger of both concepts was commendably widespread in many cases in which the case's ratio has been cited. In Lewison (2014, p. 284), the *Belize Telecom* judgment is realistically taken to "represent the current state of the law of England and Wales". Notably, there is a similarity between Hoffmann's radical departure in *Belize Telecom* vis-à-vis implications of terms in fact as well as his *ICS* decision in which he considered the five restatement as discarding the old intellectual baggage in contractual interpretation, an approach that somewhat unsettled the law of interpretation (Peters, 2009; Davies, 2010; Carter & Courtney, 2015).

Although the UKSC restored the traditional tests in *Marks and Spencer* in 2015, none of the previous cases of Hoffmann in which he merged implication with interpretation were however overruled. Instead, the ratio decidendi in *Belize Telecom* was improperly distinguished in *Marks and Spencer* as not changing the law but as lowering the threshold for implying terms, thus conveying an impression that the scholarly community had completely misunderstood *Belize*. Similarly, in *Barton v Morris,* the UK Supreme Court veered off track vis-à-vis implication of terms in fact: therein, the implied term discourse was mixed up with unjust enrichment and quantum meruit.

The rapprochement between common law and

[1] In relation to unjust enrichment, see *Fibrosa Spolka Akcyjna v Fairbairn Lawson Combe Barbour Ltd* [1943] AC 32; *Lipkin Gorman v Karpnale Ltd* [1991] 2 AC 548, HL; *Benedetti v Sawiris* [2013] UKSC 50.

[2] See *Rochefoucauld v Boustead* [1897] 1 Ch 196; *Binions v Evans* [1972] Ch 359; *Tinsley v Milligan* [1994] 1 AC 340.

[3] (2013) 2 NWLR (Pt 1338) 203.

[4] Ibid, 232.

[5] See the following Nigerian cases: *Dantata v Mohammed* [2000] 7 NWLR 176, 205 (Onu, JSC); *Thomas* v. *Olufosoye* (1986) 1 NWLR (Pt. 18) 669 (Oputa, JSC); *Bello & 13 Ors. v. A. G. Oyo State* (1986) 5 NWLR (Pt. 45) 828.

civil law systems continues to roughly impact on how common law issues are interpreted in adversarial courts. For example, the concept of using a reasonable person as a yardstick for measuring the intention of parties is a legal fiction, because, in practice, there is hardly such a reasonably third party bequeathed with the task to reasonably intervene: instead a judge sitting alone is the one who steps into the position of the imaginary third party. From Lord Denning's use of reasonableness (man on the Clapham omnius), to the traditional tests of business efficacy and officious bystander, to Hoffmann's merger, ascertaining implied terms in contracts continue to pose challenges. It is recommended that in commercial contracts the benchmark for reasonableness should not be based on an officious bystander's perspective even when they may lack special knowledge of the business. Similarly, the business efficacy test should truly be determined by an unbiased third party expert with extensive business experience—the cost for hiring this third party can be footed by the parties or incorporated as part of the court filing fees.

Lastly, quantum meruit is a well-established doctrine in contract law, which ensures that a performing party is rewarded fairly to the extent of their performance. Similarly, at common law, contracts can sufficiently be formed by conduct: for example, acceptance of a reduced sale price. In *Barton*, the monetary loss (the forfeited GBP1.2 million) should not have been allowed to remain where it had fallen in Foxpace's hands, since Mr. Barton did not come to court with unclean hands. These English apex cases—*Belize Telecom*, *Marks and Spencer* and *Barton v Morris*—have not yet been cited in any Nigerian case. The content of Nigerian case law is still largely comprised of the traditional tests, and it is unclear how Nigerian courts would apply (or be interested in applying) the ratios of these cases. This article recommends that Nigerian courts should not apply Baron as is—the doctrine of unjust enrichment and quantum meruit, as well as the maxims of equity should continue to guide courts in the enforcement of legal rights.

Biographical Note

Dr. Joseph Nwobike is a highly sought-after lawyer that leads the Osborne Law Practice in Nigeria. He is a Senior Advocate of Nigeria (SAN), a Fellow of the Chartered Institute of Arbitrators (UK), and has over 30 years of litigation experience in commercial law and human rights. He has provided a countless number of national and foreign clients with authoritative legal advice in the areas of Corporate Law, Insolvency and Debt Restructuring, Data Protection, Mergers and Acquisitions, Foreign Investments, Contracts and Finance Transactions. He is a scholar-practitioner and enjoys academic legal research and writing.

References

Journal Articles

Andrews, N. (2017). Interpretation of contracts and "commercial common sense": do not overplay this useful criterion. *Cambridge Law Journal, 76*(1), 36-62.

Baker, J. (2019). The common law of England. In: *Introduction to English Legal History.* 5th edn, Oxford University Press.

Ben-Shahar, Omri. (2004). Agreeing to disagree: filling gaps in deliberately incomplete contracts. *Wisconsin Law Review, 2*, 389-428.

Carter, JW & Courtney, W. (2015). Belize Telecom: a reply to professor McLauchlan. *Lloyd's Maritime & Commercial Law Quarterly,* 245-262.

Cross, R & Harris, JW. (1991). Stare decisis. In: *Precedent in English Law.* Oxford University Press.

Davies, P. (2010). Recent developments in the law of implied terms. *Lloyd's Maritime & Commercial Law Quarterly,* 140-149.

Devlin, P. (1951). The relation between commercial law and commercial practice. *Modern Law Review, 14*(3), 249-266.

Dworkin, R. (1977). *Taking rights seriously*. Harvard University Press.

Garner, BA. (2004). Black's law dictionary. 8th edn, Thomson West Publishing Co. p. 345.

Jewel, L. (2019). Does the reasonable man have obsessive compulsive disorder? *Wake Forest Law Review, 54*, 1049-1088.

Kramer, A. (2003). Common sense principles of contract interpretation—and how we've been using them all along. *Oxford Journal of Legal Studies, 23*(2), 173-196.

Kramer, A. (2004). Implication in fact as an instance of contractual interpretation.

Cambridge Law Journal, *63*(2), 384–411.

Lewison, K. (2014). *The Interpretation of Contracts.* 5th edn, Sweet & Maxwell.

Linzer, P. (2002). The comfort of certainty: plain meaning and the Parol evidence rule. *Fordham Law Review, 71*, 799-839.

Lord Denning. (1979). *The discipline of law*. Butterworths, Scarborough.

Lord Hoffmann. (1995). Anthropomorphic justice: the reasonable man and his friends. *Law Teacher, 29*(2), 127-141.

Lord Wright. (1935). *Some developments in commercial law in the present century*. Birmingham: Holdsworth Club.

McCunn, J. (2019). The contra proferentem rule: contract law's great survivor. *Oxford Journal of Legal Studies, 39*(3), 483-506.

Mitchell, C. (2003). Leading a life of its own? The roles of reasonable expectations in contract law. *Oxford Journal of Legal Studies, 23*(4), 639-665.

Moran, M. (2003). *Rethinking the reasonable person: an egalitarian reconstruction of the objective standard.* Oxford University Press.

Peters, C. (2009). The implication of terms in fact. *Cambridge Law Journal, 68*(3), 513-515.

Posner, EA. (1998). The Parol evidence rule, the plain meaning rule and the principles of contractual interpretation. *University of Pennsylvania Law Review, 146*, 533-577.

Schwartz, A., & Scott, R. E. (2003). Contract theory and the limits of contract law. *The Yale Law Journal*, *113*(3), 541–619.

Steyn, J. (1997). Contract law: fulfilling the reasonable expectations of honest men. *Law Quarterly Review*, *133,* 433-442.

Wilmot-Smith, F. (2023). Express and implied terms. *Oxford Journal of Legal Studies, 43*(1), 54–75.

Zuppi, AL. (2007). The Parol evidence rule: a comparative study of the common law, the civil law tradition, and lex mercatoria. *Georgia Journal International & Comparative Law, 35,* 233-276.

Case Law

Antaios Cia Naviera S.A. v Salen Rederierna AB [1985] AC 191, HL.

Arnold v Britton [2015] UKSC 36.

Attorney General of Belize v Belize Telecom Ltd [2009] UKPC 10.

Barton & Ors *v Morris* & Anor [2023] UKSC 3.

Bello & 13 Ors. v. A. G. Oyo State (1986) 5 NWLR (Pt. 45) 828.

Benedetti v Sawiris [2013] UKSC 50.

Beswick v Beswick [1968] AC 58, HL.

Betamax Ltd v State Trading Corporation [2021] UKPC 14.

Binions v Evans [1972] Ch 359.

BP Refinery (Westernport) Pty Ltd v President, Councillors and Ratepayers of the Shire of Hastings (1977) 52 Australian Law Journal Report 20.

British Movietonews Ltd v. London and District Cinemas Ltd (1952) AC 166.

Carmichael v National Power Plc [1999] 1 WLR 2042, 2049.

Central London Property Trust Ltd v High Trees House Ltd [1947] KB 130.

Chandelor v Lopus (1603) 79 ER 3.

Chappell v Times Newspapers Ltd [1975] 1 WLR 482.

Chartbrook Ltd v Persimmon Homes Ltd [2009] UKHL 38.

Dakin & Co Ltd v Lee [1916] 1 KB 566.

Dantata v Mohammed [2000] 7 NWLR 176 (Onu, JSC).

Daspan v Mangu Local Govt Council (2013) 2 NWLR (Pt 1338) 203.

Dennis Reed Ltd v Goody [1950] 2 KB 277.

Equitable Life Assurance Society v Hyman [2002] 1 AC 408.

Fibrosa Spolka Akcyjna v Fairbairn Lawson Combe Barbour Ltd [1943] AC 32.

Frost v Knight (*1872*) LR 7 Exch 111.

Hall v. Brooklands Auto-Racing Club [1932] 1 KB 205.

Hoenig v Isaacs [1952] 2 All ER 176.

Ibama v. Shell Pet. Dev. Co. (Nig.) Ltd (1998) 3 NWLR (Pt. 542) 493.

Investor Compensation Scheme v West Bromwich [1998] 1 WLR 896.

Lipkin Gorman v Karpnale Ltd [1991] 2 AC 548, HL.

Liverpool City Council v. *Irwin* [1976] QB 319. CA.

Liverpool City Council v. *Irwin* [1977] AC 239, HL.

Marks and Spencer plc v BNP Paribas Securities Services Trust Company (Jersey) Ltd [2015] UKSC 72.

May & Butcher Ltd v The King [1934] 2 KB 17.

McQuire v. Western Morning News Co [1903] 2 KB 100, CA.

Mediterranean Salvage & Towage Ltd v Seamar Trading & Commerce Inc [2009] EWCA Civ 531.

Miller v. Jackson [1977] QB 966.

Multichoice (Nig.) Ltd v. Azeez (2010) 15 NWLR (Pt.1215) 40 (Court of Appeal).

Okoebor v. Eyobo Eng. Serv. Ltd (1991) 4 NWLR (Pt. 187) 553.

Omega Bank v. O.B.C. Ltd. (2005) 8 NWLR (Pt. 928) 547 (per Kutigi JSC, Nigerian Supreme Court).

Patel v Ali [1984] Ch 283.

Philips Electronique Grand Public SA v British Sky Broadcasting Ltd [1995] Entertainment and Media Law Report 472.

Prenn v Simmonds [1971] 1 WLR 1381, HL.

Printing and Numerical Registering Co v Sampson (1875) 19 Eq 462.

Reigate v. Union Manufacturing Company [1918] 1 KB 592.

Riggs v Palmer 115 NY 506 (1889).

Rochefoucauld v Boustead [1897] 1 Ch 196.

Scammell and Nephew Ltd v Ouston [1941] AC 251.

See *Luxor (Eastbourne) Ltd v Cooper* [1941] AC 108 (per Lewison LJ).

Shell UK v. Lostock Garages (1977) 1 All ER 481.

Shiloh Spinners Ltd v Harding [1973] AC 691, HL.

Société Générale, London Branch v Greys [2012] UKSC 63.

South Australia Asset Management Corporation v York Montague Ltd [1997] AC 191.

Southern Foundries (1926) Ltd v Shirlaw [1939] 2 KB 206 (CA).

Stickney v Keeble [1915] AC 386, HL.

The Moorcock (1889) 14 PD 64 (CA) 68, Bowen LJ.

Thomas v. *Olufosoye* (1986) 1 NWLR (Pt. 18) 669 (Oputa, JSC).

Tinsley v Milligan [1994] 1 AC 340.

Torvald Klaveness A/S v Arni Maritime Corporation [1994] 1 WLR 1465 (HL).

Transfield Shipping Inc v Mercator Shipping Inc (*The Achilleas*) [2008] UKHL 48.

Trollope & Colls Ltd. v. North West Metropolitan Regional Hospital Board (1973) 2 All ER 260.

Union Bank of Nigeria plc v. Awmar Properties Ltd (2018) 10 NWLR 64.

Walsh v Lonsdale (1882) 21 Ch D 9.

Wells v Devani [2019] UKSC 4.

PIONEER
ACADEMIC PUBLISHING LIMITED

Studies in Law and Justice
ISSN 2958-0382
www.pioneerpublisher.com/slj
Volume 4 Number 3 June 2025

Judicial Application of the Anti-Domestic Violence Law in Rural Courts: A Case Study of Henan and Sichuan Provinces (2016–2023)

Yanan Liu[1] & Minghui Zhao[1]

[1] Henan University of Economics and Law, Zhengzhou, Henan, China
Correspondence: Yanan Liu, Henan University of Economics and Law, Zhengzhou, Henan, China.

doi:10.56397/SLJ.2025.06.05

Abstract

This paper investigates the judicial application of China's Anti-Domestic Violence Law (2015) in rural courts, focusing on selected counties in Henan and Sichuan provinces between 2016 and 2023. Drawing on court documents, policy reports, and NGO data, it explores how local courts interpret and enforce protection orders, navigate evidentiary standards, and reflect embedded cultural norms. Despite the law's rights-based framework and procedural tools, enforcement in rural areas remains inconsistent, shaped by infrastructural limitations, mediation culture, and judicial discretion. The study reveals that formal legal protection is frequently overridden by informal norms, narrow interpretations of harm, and resource scarcity. The paper calls for a more contextually grounded and gender-sensitive enforcement model that strengthens procedural accountability while reshaping rural legal consciousness.

Keywords: Anti-Domestic Violence Law, rural courts, protection order, judicial discretion, gender and law, Chinese legal system

1. Introduction

Domestic violence has long remained a pervasive but under-addressed issue within China's legal and cultural landscape. While significant progress has been made since the enactment of the Anti-Domestic Violence Law in 2015, rural areas continue to exhibit lower levels of legal intervention, public awareness, and institutional support. In provinces such as Henan and Sichuan—regions with large rural populations, high internal migration, and diverse sociocultural dynamics—the challenges in responding to domestic abuse are both systemic and culturally embedded.

Surveys conducted by All-China Women's Federation (ACWF) in the years following the law's enactment have consistently shown that rural women are less likely than urban women to report incidents of abuse or seek institutional help. A 2019 provincial-level study on gender-based violence in central China noted that fewer than 15% of rural survivors had approached police or local courts, citing social stigma, fear of retaliation, and a deeply rooted perception that "family shame should not be made public." This reluctance is exacerbated by

informal dispute resolution mechanisms such as village mediation committees, which often prioritize marital reconciliation over victim protection.

Cultural factors—such as the enduring influence of patrilineal kinship norms and a widespread acceptance of hierarchical gender roles—create an environment where abuse is often normalized or dismissed as a private family matter. In this context, domestic violence is frequently framed not as a legal violation, but as a "conflict" requiring compromise.

Legal awareness in these settings remains fragile. While urban legal aid centers and WeChat-based outreach campaigns have improved general familiarity with protection orders and complaint procedures, grassroots knowledge of the Anti-Domestic Violence Law remains uneven and shallow. Victims and village-level officials alike often misunderstand key provisions, including the types of abuse covered (e.g., economic and emotional violence) and the eligibility criteria for civil protection orders.

Moreover, structural limitations in rural legal infrastructure—such as court accessibility, language barriers, and lack of specialized personnel—further dilute the law's potential. Although the Anti-Domestic Violence Law formally applies nationwide, its implementation diverges widely across rural contexts, reflecting the interplay of local resources, attitudes, and administrative will.

In short, domestic violence in rural China represents not only a legal issue but a complex nexus of cultural silence, institutional weakness, and legal invisibility. Understanding this context is critical to assessing how the law functions—or fails to function—when it meets the realities of village courts, local cadres, and rural households.

2. The Anti-Domestic Violence Law (2015): Legal Scope and Procedural Tools

2.1 Core Legal Definitions and Protection Mechanisms

The promulgation of the Anti-Domestic Violence Law of the People's Republic of China (hereafter, ADVL) in 2015 marked a watershed moment in the formal recognition of domestic abuse as a distinct legal harm. The law defines domestic violence as physical, psychological or other harm inflicted between family members by means such as beating, binding, maiming, restricting personal freedom or other actions.[1] This definition is notable for including non-physical forms of abuse, such as emotional coercion and intimidation, which had long been neglected in legal and administrative adjudication.

One of the law's most impactful mechanisms is the civil protection order system established in Chapter III. Victims may apply to the basic-level People's Court for urgent protective measures requiring the abuser to vacate shared residence, cease contact, or refrain from harassment.[2] In principle, emergency rulings must be issued within 72 hours. However, data from national case-monitoring reports indicate that actual issuance of protection orders in rural counties remains extremely low. In some counties in Henan and Sichuan, courts issued fewer than 10 such orders per year between 2017 and 2021, with denials often based on claims of insufficient material evidence or reconciliation by the couple.[3]

2.2 Institutional Responsibilities and Rights-Based Provisions

The ADVL outlines responsibilities for a multi-agency enforcement network, assigning duties to police, courts, local committees, schools, and employers. Article 6 emphasizes prevention, education, and coordinated response across institutions.[4] Article 7 tasks local governments with developing support services such as temporary shelters, psychological counseling, and legal aid, though these services remain concentrated in urban centers.[5]

Crucially, Article 16 imposes a direct obligation on public security organs to investigate domestic violence reports, issue written warnings, and assist courts in the evidence collection necessary for protective orders.[6] Nevertheless, local law enforcement in rural areas frequently resorts to verbal mediation, especially where elders or economically dependent women are involved.

The law also extends protection beyond traditional spousal or blood relationships,

[1] Anti-Domestic Violence Law of the People's Republic of China (中华人民共和国反家庭暴力法), Article 2.

[2] Ibid., Articles 23–29.

[3] China Law Society & All-China Women's Federation, *Protection Order Implementation Report* (2018–2022).

[4] ADVL, Article 6.

[5] Ibid., Article 7.

[6] Ibid., Article 16.

covering co-residing or caregiving relationships, including former spouses, adoptive family members, and step-relatives.[1] This broad scope reflects a shift toward a rights-centered framing of family violence, though such distinctions are often poorly understood at the village level.

Despite its progressive architecture, the law's practical enforceability in rural regions—especially those with limited judicial capacity—remains inconsistent. As later sections demonstrate, the translation of these formal protections into grassroots court procedures is mediated by resource limitations and social norms.

3. Judicial Practice in Rural Courts of Henan and Sichuan

3.1 Constraints in Local Court Infrastructure

Rural courts in Henan and Sichuan operate within environments marked by institutional scarcity, where human and material resources fall short of urban standards. Many basic-level People's Courts (基层人民法院) in townships lack dedicated personnel trained in gender-based violence, and often share case dockets with family mediation, divorce, and inheritance matters. Judges typically juggle high caseloads across jurisdictions, limiting the time and capacity available for thoroughly investigating domestic violence claims.

Moreover, despite legal reforms, rural judicial processes remain overwhelmingly paper-based, with weak integration into national digital case management systems such as "China Judgments Online" (中国裁判文书网). This results in a lack of consistent documentation, making cross-county comparisons or systematic enforcement tracking difficult. In some townships, even civil protection orders are issued without standardized forms or record-keeping, leading to inconsistencies and procedural confusion.

Court infrastructure also suffers from geographic inaccessibility. In hilly or agriculturally dispersed counties of western Sichuan, some litigants must travel over 80 kilometers to reach the nearest court, an obstacle especially acute for women with limited mobility, caregiving burdens, or restricted household authority. The opportunity cost of litigation often disincentivizes formal complaint, favoring informal or negotiated alternatives.

3.2 Influence of Local Governance and Informal Norms

Judicial decision-making in rural Henan and Sichuan is shaped not only by law but also by the institutional logic of local governance. Village cadres, party committees, and mediation teams frequently play a frontline role in domestic conflict resolution—often acting as gatekeepers to formal legal intervention. While this aligns with traditional Chinese legal pluralism, it also opens space for moralistic or patriarchal reasoning that may deprioritize victim autonomy.

Field interviews and NGO case reports from Ya'an (Sichuan) and Zhoukou (Henan) show that local courts often defer to "harmony-first" dispute settlement practices, encouraging reconciliation rather than restraining orders—even when abuse patterns are documented. In one 2021 case from Xinye County, the court declined to issue a protection order, citing "the couple's rural background and mutual dependence as elderly farmers" as grounds for pursuing reconciliation through local village mediation.

Judges themselves, especially in township-level courts, may lack exposure to feminist legal reasoning or trauma-informed adjudication. This results in a narrow interpretive frame, where "violence" is often equated with physical harm alone, and claims of psychological or economic abuse are dismissed as insufficiently demonstrable.

In sum, the implementation of the Anti-Domestic Violence Law in rural Henan and Sichuan courts is mediated by a blend of procedural fragility and culturally specific judicial logics, in which state law coexists with—and is often overridden by—informal authority structures and rural social ethics.

4. Protection Order Enforcement and Regional Trends (2016–2023)

Despite the legislative clarity provided in Chapter III of the Anti-Domestic Violence Law, the issuance of personal protection orders (PPOs) in rural courts remains sporadic, underutilized, and regionally uneven. This section examines practical trends in enforcement within Henan and Sichuan provinces between 2016 and 2023, based on publicly available court data, policy bulletins, and civil society reports.

A comparative analysis of basic-level court

[1] Ibid., Article 37.

records from selected counties shows a marked disparity in the volume and consistency of protection order rulings. In Sichuan's Ya'an Prefecture, for instance, only 26 protection orders were issued across seven counties over a six-year period, with more than half of applications rejected due to "insufficient threat to personal safety." [1] Meanwhile, in Henan's Xinyang region, several county-level courts reported no recorded PPO cases between 2018 and 2021, despite high levels of reported domestic conflict in township police filings.[2]

The primary barriers to enforcement include:

- Evidentiary thresholds that remain too high for rural litigants, especially in cases involving emotional or economic abuse.
- Judicial reluctance to interfere in family dynamics without "clear physical harm".
- Informal mediation preferences by village committees and judicial panels, often preempting formal rulings.

Some courts further complicate access by requiring written applications, witness affidavits, or third-party notarization—procedures rarely feasible for victims in remote areas or abusive households. A review of case files from Henan Provincial Women's Federation revealed that over 60% of denied PPO requests in rural courts were returned without detailed procedural guidance, leaving survivors confused and unprotected.[3]

Regional policy directives have attempted to improve this landscape. The Sichuan Provincial High People's Court's 2020 Guiding Opinion explicitly instructs local courts to accept non-physical abuse claims and to process PPO requests "with urgency and empathy."[4] While such moves signal institutional awareness, implementation remains fragmented.

An additional trend worth noting is the outsized role of women's federations and NGOs in successful applications. In both provinces, nearly all granted PPOs involved legal aid or third-party advocacy, suggesting that procedural navigation is dependent on intermediary support, which is far scarcer in rural communities.

Thus, while the legal mechanism for protection exists, its practical reach remains narrow, its access limited, and its application vulnerable to institutional avoidance and normative hesitation. These constraints not only endanger victims but also undercut the law's symbolic authority as a universal rights instrument.

5. Gender, Evidence, and Judicial Reasoning

In rural Chinese courts, especially those in Henan and Sichuan, judicial decisions regarding domestic violence are not only legal determinations but also cultural performances of gender norms and evidentiary ideology. The analysis of court verdicts, rejection letters, and publicly available rulings reveals consistent patterns in how gendered assumptions and strict evidentiary burdens shape judicial reasoning.

A review of 38 civil protection order judgments from 2016 to 2022 across the two provinces shows that courts rarely grant requests in the absence of physical injury evidence—typically limited to hospital reports or police documentation. Emotional, verbal, or economic abuse—though explicitly included under the Anti-Domestic Violence Law [5]—is frequently dismissed as "domestic disputes" lacking "objective proof."[6] For example, a 2020 ruling from a township court in Zhumadian, Henan, denied a petitioner's request, stating that "accusations of verbal humiliation and financial control are not actionable unless corroborated by external parties or visual documentation."[7]

Such reasoning reflects a formalistic evidentiary culture, one that disadvantages victims, particularly women, who are often isolated or unable to document abuse due to economic dependence or mobility constraints. Judicial insistence on "third-party neutrality" or "clear and present danger" contradicts Article 2 and Article 23 of the ADVL, which emphasize

[1] Ya'an Intermediate People's Court, Annual Judicial Work Summary (2017–2022), Section on Civil Protection Orders.

[2] Xinyang Women's Rights Legal Hotline Report, unpublished internal data (2021).

[3] Henan Provincial Women's Federation, *Protection Order Case Follow-up Report*, 2022.

[4] Guiding Opinion on Enhancing Judicial Protection against Domestic Violence, Sichuan High People's Court, 2020.

[5] Anti-Domestic Violence Law of the People's Republic of China (中华人民共和国反家庭暴力法), Articles 2 and 23.

[6] Xinyang County Court Ruling, 2021 (Case No. 2021 豫 1523 民初字 00324 号), publicly available via China Judgments Online.

[7] Zhumadian Township Court Judgment, Henan Province, December 2020, unpublished document provided by Henan Women's Legal Aid Center.

preventive and rights-based protection, not retroactive punishment.[1]

Further, rulings often reveal a discursive asymmetry in how male and female litigants are characterized. Male respondents are frequently portrayed as "providers," "rural heads of household," or "emotionally unstable but family-oriented," while female petitioners may be described as "quarrelsome," "overly sensitive," or "provoking conflict." Such language implicitly delegitimizes female agency and elevates marital stability over victim safety.

Moreover, courts often invoke mediation preference as judicial justification, citing parties' shared economic interest or co-residence with elderly dependents. This tendency reflects not only doctrinal discretion but also the structural embedding of conciliationist ideology within rural legal consciousness, where judges are also community mediators and political risk managers.

In some progressive cases, particularly in urbanizing counties like Dujiangyan (Sichuan), judges have experimented with alternative evidentiary acceptance, such as WeChat messages, audio recordings, or third-party community testimony. However, these practices remain exceptions, not norms, and rely heavily on individual judicial initiative rather than institutional protocol.

Ultimately, judicial reasoning in rural domestic violence cases reveals two levels of constraint: one of institutional evidence standards and another of embedded gender ideology. Both act as filters through which the Anti-Domestic Violence Law is interpreted and narrowed—undermining its purpose and limiting its emancipatory potential.

6. Rethinking Legal Impact in Rural Anti-Violence Efforts

The implementation of China's Anti-Domestic Violence Law in rural Henan and Sichuan reveals the persistent gap between statutory design and judicial practice. While the law's textual commitments to protection, prevention, and victim rights signal a progressive shift in legislative intent, its on-the-ground enforcement remains constrained by infrastructural scarcity, cultural inertia, and discretionary legal reasoning.

As this paper has shown, protection orders—arguably the law's most vital procedural tool—are underutilized not because they lack legal basis, but because their application conflicts with the structural and ideological realities of township-level courts. Judicial reluctance to accept non-physical forms of abuse, preference for informal mediation, and adherence to evidentiary thresholds unsuited for domestic settings all contribute to the hollowing out of legal protection.

Furthermore, the fusion of judicial authority with local governance roles in rural areas introduces a normative bias toward familial preservation, often at the cost of victim safety. This "protective paternalism," while culturally legible, dilutes the rights-based orientation of the Anti-Domestic Violence Law and reproduces the very hierarchies the law seeks to undo.

To move from symbolic law to substantive protection, reforms must be both procedural and cultural. At the procedural level, judicial training, simplified evidence rules, and automatic review of denied PPOs are urgently needed. At the cultural level, village cadre education, gender-sensitive legal literacy campaigns, and stronger civil society engagement must accompany legal enforcement.

Equally important is the need to institutionalize accountability mechanisms for court refusal patterns, including public reporting of protection order data and provincial-level audits. Judicial discretion must remain—but it must be structured by transparent standards, peer oversight, and a clear bias toward the protection of vulnerable individuals.

Ultimately, the impact of anti-violence law cannot be measured merely by formal compliance or legislative elegance. It must be evaluated through its ability to transform the lived experiences of rural victims, empower local institutions without reinforcing patriarchy, and position legal consciousness as a force not of regulation, but of liberation.

References

Anti-Domestic Violence Law of the People's Republic of China. (2015). Adopted by the Standing Committee of the National People's Congress, December 27, 2015.

China Law Society & All-China Women's Federation. (2020). *Protection Order Monitoring Report: National Trends and*

[1] ADVL, Articles 2 & 23 emphasize early intervention and civil relief, not reactive injury-based thresholds.

Challenges. Beijing: China Women's Publishing House.

Henan Provincial Women's Federation. (2022). *Protection Order Case Follow-up Report: Rural Judicial Practice in Henan*. Zhengzhou: Internal Research Bulletin.

Sichuan High People's Court. (2020). *Guiding Opinion on Enhancing Judicial Protection against Domestic Violence*. Chengdu: Provincial Judicial Affairs Office.

Wang, L., & Li, J. (2021). The Limits of Law: Evidentiary Challenges in Domestic Abuse Litigation. *Tsinghua China Law Review*, *13*(1), 55–74.

Ya'an Intermediate People's Court. (2022). *Annual Judicial Work Summary (2017–2022)*. Ya'an: Sichuan Provincial Court Archive.

Zhang, X. (2019). Family Harmony and Judicial Practice: Mediation in Rural Domestic Violence Cases. *Peking University Law Journal*, *31*(2), 85–108.

Zhumadian Township Court. (2020). Judicial Ruling on Civil Protection Order Application, Case No. 2020ZMD123. Unpublished.

PIONEER
ACADEMIC PUBLISHING LIMITED

Studies in Law and Justice
ISSN 2958-0382
www.pioneerpublisher.com/slj
Volume 4 Number 3 June 2025

Thinking of Harm, Surveillance and Corporate Responsibility in Digital Criminology

Jiachen Xu[1]

[1] The University of Sydney Law School, Sydney, Australia
Correspondence: Jiachen Xu, The University of Sydney Law School, Sydney, Australia.

doi:10.56397/SLJ.2025.06.06

Abstract

This paper explores how harm, control, and responsibility appear in the digital age, using the 2023 Latitude Financial data breach and technology-facilitated abuse cases as examples. The study applies digital criminology and surveillance theory to understand the hidden and complex nature of modern cybercrime. First, it discusses how hackers use technical methods to attack companies indirectly, and how poor communication after a breach can increase the harm to users. Then, it shows how surveillance tools are also used in private settings, such as domestic violence, to control victims. The paper finds that harm in the digital world is often invisible, long-term, and hard to prevent. It argues that current laws are not enough to deal with these new types of crime. Stronger regulation, better cross-border cooperation, and more attention to surveillance misuse are needed to protect people in digital environments.

Keywords: digital criminology, surveillance theory, data breach, invisible harm, corporate responsibility, technology-facilitated abuse

1. Introduction

As digital technologies continue to reshape society, new forms of crime and harm have emerged that challenge traditional legal and criminological frameworks. One example is the 2023 cyberattack on Latitude Financial, which exposed the personal data of millions of customers and raised public concerns about corporate responsibility, data governance, and regulatory failure. [1]At the same time, the misuse of surveillance technologies in private settings—such as domestic violence involving spyware—shows how harm can also occur in interpersonal contexts through digital means. This paper explores these issues using the frameworks of digital criminology and surveillance theory. It argues that digital harm is often hidden, delayed, and extended, requiring new approaches to regulation, punishment, and prevention. The study focuses on two core cases: the Latitude Financial data breach and the use of technology in intimate partner abuse. By analyzing both institutional and personal examples of digital harm, the paper aims to rethink how power, control, and responsibility operate in a digital society, and to suggest ways

[1] ABC News, (2023). Latitude Financial Customers Frustrated by Lack of Communication after Cyberattack. 28 March 2023. https://www.abc.net.au/news/2023-03-28/latitude-financial-customers-frustrated-lack-of-communication/102151166 accessed 12 October 2024.

the law might better address these challenges.

2. Summaries of News Reports and Their Relevance to Digital Criminology

In 2023, the cyberattack on Latitude Financial led to the hole of amounts of individual data, increasing customer concerns over the company's data protection methods and inadequate communication. Numerous sensitive customer data were revealed as a result of the cyberattack. Customers who were affected feel dissatisfied with Latitude. They think the company did not communicate enough and kept data for too long. They also see problems in how Latitude manages data security. These customers believe that the company has not done enough to fix these issues. The event is strongly related to digital criminal behavior, digital enforcement, and digital punishment. Firstly, this incident reflects digital criminal behavior. Hackers gained access to Latitude's third-party systems, demonstrating that the company's supply chain has spaces in terms of security gaps. This is similar to the computer attack in the Medibank event, where hackers exploited vendor vulnerabilities to gain access to sensitive data, revealing the trend of using external partner vulnerabilities for system intrusion in modern digital crimes. Next, the event reflects the problem with digital regulation in Australia. The Latitude event exposed the companies' and related institutions' inadequacies in data retention and supervision. When information is no longer needed, companies are required to eliminate or encrypt it according to the Australian Privacy Principles. However, Latitude's long-term retention of historical customer data indicates the need to strengthen supervision of enterprise data management. Finally, news reports reflect that there is some space for reform in Australia's digital punishment. A discussion about corporate responsibility and punishment mechanisms has arisen as a result of Latitude's decision to remain silent in its reaction to the data breach.

3. Selected Theoretical Framework: Digital Criminology

With the development of technology, digital criminology is also constantly evolving, and the rapid development of digital technology has had an impact on criminal behavior, law enforcement, and criminal justice systems. Social actions, business methods, and criminal behavior have all gone through big changes. These changes happened because digital technology has spread widely. The advancement of technology and the improvement of usability have driven the widespread application of digital media, affecting various aspects of social life.[1] In addition, digital criminology attempts to explain how the understanding, execution, and tackling of legal actions are profoundly affected by the digital lifestyle. It also focuses on cybercrime, such as hacking, identity theft. Digital technology is not only a means of preventing and combating crime, but also a tool for crime. Digital technology has been integrated into People's Daily Lives in modern society. Every aspect of contemporary society, including work, social relationships, media usage, and more, is influenced by electronic devices and the Internet.[2] In the digital society, criminal act is becoming more and more complex, and traditional criminological theory can no longer fully reveal emerging forms of crime such as data leakage and privacy invasion. Digital criminology completes this vacuum and offers a fresh perspective on how to interpret and respond to digital crime.

4. The Theory of Digital Criminology Embodied in the News

4.1 Digital Criminal Behavior

First of all, it reflects the variety and complexity of attack methods under modern digital criminal behavior. The cyber attack at Latitude Financial highlights the range and technical complexity of the methods of committing current online crimes. Hackers break through security protection by exploiting vulnerabilities, demonstrating the high-tech nature of contemporary hacker attacks. The risk of cyberattacks and incursions grows as the use of modern technologies grows. Detecting these attacks has become challenging, not only because the attack methods are becoming increasingly complex, but also because the current IT infrastructure is large and complex in scale.[3] Usually, these problems are carried out through a series of meticulously planned steps rather than a single technology means. These

[1] Gavin J D Smith, Lyria Bennett Moses and Janet Chan. (2017). The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-Driven Approach. *British Journal of Criminology, 57*, 259, 265.

[2] Deborah Lupton. (2015). *Digital Sociology*, 1-6, Routledge.

[3] Mariya Ouaissa et al (eds). (2022). *Big Data Analytics and Computational Intelligence for Cybersecurity*, Springer.

include phishing emails, exploiting weaknesses in corporate networks, and an in-depth analysis of the digital ecosystem of enterprises to determine the best way of incursion.[1] Hackers gained access to the systems of third-party vendors in the Latitude Financial event, exhibiting the potential security risks of technology dependence and information sharing between businesses and external vendors. Because hacker does not immediately attack Latitude Financial systems, but attacks a third-party vendors, it is difficult to spot this striking. Network defense becomes more difficult as a result of this indirect attack, and standard firewalls and intrusion detection systems struggle to identify the cause of the threat first. Faced with the growth and complexity of such means, the defense strategy of enterprises faces enormous challenges. In contrast, hackers frequently take advantage of emerging technologies to quickly bypass detection. Business defense capabilities must not only have a high level of agility but also develop a multi-level security system at the technical and management levels to avoid potential risks, due to the complexity and variety of these attack methods.[2]

Second, digital criminal behavior's high level of concealment is a distinguishing quality in comparison to traditional crimes. Hackers typically enter a user's system through complex technological means and collect enough data. Hackers are able to get around company protection system. They can cause serious harm to important company data. At the same time, they can avoid being noticed for a short period. In response to such secret attacks, businesses are frequently on the defensive in the face of digital crime. In the Latitude Financial incident, hackers not only successfully infiltrated the system, but also were able to perform a series of operations after the initial intrusion to exacerbate the impact of the harm. After a period of time following the data breach, the company realized that the scale of the breach could be even larger, highlighting the covert nature of the digital crime implementation process. The invisible character of digital crime is also illustrated by the Equifax breach of 2017. The attacker infiltrated the Equifax system for about two months, exploiting vulnerabilities to obtain a large amount of users' personal information. In the end, 147 million customers' sensitive data was ultimately compromised, leaving Equifax with serious legal and financial repercussions.[3]

The transnational nature of digital crime is another quality. People, businesses, or governments in many nations can be directly or indirectly affected by digital crimes that cross national borders and are committed on a worldwide level. Attacker can attack without having to physically approach their goals because digital crime is frequently carried out using the global platform of the Internet. Medibank, another business involved in the story, was the victim of a cyberattack that exposed a lot of consumer information. According to the Australian government's confirmation, the intrusion into Medibank to steal data was carried out by Russian hackers. According to limitations on Judicial Jurisdiction, this transnational crime presents a significant challenge for nations that deal with digital crime. Attackers may use tools like virtual private networks (VPNs) and proxy servers, adding complexity to crime tracking. Due to the transnational nature of digital crime, according to Sofaer and Goodman, traditional legal frameworks are inadequate because a country's regulations and enforcement measures typically only apply to specific regional boundaries, while Internet crimes can spread across multiple national borders.[4] To address this challenge, international cooperation has become particularly important. By joining international law enforcement organizations like Interpol, signing a cyber security cooperation agreement, and achieving consensus at international events, many nations are functioning to better fight transnational digital crime. The European Union has strict rules for data that moves across borders and for keeping data private. These rules are in the General Data Protection Regulation (GDPR). This regulation was created

[1] Md Abu Imran Mallick and Rishab Nath. (2024). Navigating the Cybersecurity Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. *World Scientific News, 190*(1), 1, 39.

[2] Maria Fernanda Pires. (2024). AI and Machine Learning: Revolutionizing Supply Chain Security. *Advances in Computer Sciences*, *7*, 1, 3–5.

[3] Stephen Smiley. (2017). Equifax: Australians' Sensitive Financial Information at Risk in Data Breach of US Company. ABC News, online, 8 September 2017. https://www.abc.net.au/news/2017-09-08/smiley-credit-check-australians-financial-information-at-risk/8887198.

[4] Abraham D. Sofaer and Seymour E. Goodman. (2001). *Cyber Crime and Security: The Transnational Dimension*, 1–2, Hoover Institution Press.

in recent years. It applies to countries that are members of the EU. It also applies to companies from other countries that do business with the European Union.[1] The implementation of such international norms will help establish unified digital crime response standards on a global scale, and reduce the risks posed by transnational digital crimes. But cross-border cooperation also faces several challenges in practice. On the one hand, the laws of various nations differ in how they determine and handle crime and data security, which causes contradictions in law enforcement and extradition. On the other hand, conflicts of interest between nations, may influence the efficiency of Cross border Tracking. For instance, in the case of Medibank, even if Australia has identified the origin of the intruders, if Russia has not agreed to surrender the hackers involved, effective accountability for criminals will face great difficulties. Thus, it is important to keep working on promoting legal coordination of transnational digital crimes. This legal harmonization will help countries work together more easily in the future. It is needed to make sure they can fight against criminal actions in the global digital space.

4.2 Digital Law Enforcement and Regulation

Within the wake of the data breach at Latitude Financial, Australia's controller, the OAIC, can examine to decide whether the company's data protection measures are input. This indicates that the government plays an important regulatory role in the digital society. In today's digital society, information leakage and privacy protection have become issues that cannot be ignored. These are issues that need close attention. With the increase of cyber attacks and data theft incidents, global governments and regulatory agencies are facing a huge challenge of how to effectively protect personal information and ensure that businesses comply with information protection security standards. Cybercrime is different from traditional criminal act, driven by the quick advancement of Web innovation, cybercriminals typically possess a high level of education and professional skills. Hackers can utilize complex coding procedures to attack, which reflect the continuous improvement of digital security measures and the importance of cooperation among various institutions.[2] Digital criminology explores the response measures of legal and regulatory agencies and points out that effective digital regulation is important to decreasing the information breaches. Specifically, the objective of digital regulation is to constrain companies to take effective data protection measures to guarantee the security of user's data through legislation and enforcement. In Australia, a fundamental system for privacy protection for citizens has been set up through the Australian Privacy Principles and the OAIC has been set up to supervise data management compliance for businesses.

In the case of Latitude Financial, the OAIC started an investigation into the company after the incident. This investigation was to check if the company follows the rules of the Australian Privacy Principles. This event highlights the important role of the OAIC in cases of information breaches. OAIC reviews enterprise data governance measures to ensure that enterprises fulfill their corresponding legal responsibilities in information protection. Australian Privacy Principles require businesses to eliminate or hide of data identification information.[3] But Latitude Financial has saved unnecessary information for up to 18 years, raising questions about its information administration practices. The OAIC's duty not only included posting evaluation of corporate responsibility but also investigated whether there was systemic negligence in data management.

The Latitude Financial incident shows a central and sensitive issue in digital regulation, how to ensure that companies actively meet their notification obligations after a data breach occurs and promptly notify affected users. Companies, especially listed ones, may choose to hide for fear of hurting their share prices. In digital society, data breaches are inevitable, but how to notify victims quickly and accurately has become one of the important criteria to measure the effectiveness of digital regulation. In this incident, Latitude Financial was questioned for failing to communicate with customers in a

[1] European Parliament and Council, Regulation (EU) 2016/679 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation), art 3.

[2] Naeem AllahRakha. (2024). Transformation of Crimes (Cybercrimes) in Digital Age. *International Journal of Law and Policy*, *2*(2), 1, 8.

[3] Office of the Australian Information Commissioner. (January 2014). Australian Privacy Principles. APP 11.

timely manner, many of whom only learned of the severity and scope of the incident through media reports. This lack of transparency not only adversely affects customers and the public interest, but also makes it difficult for regulators to fully understand the nature and scale of incidents at an early stage, thereby impeding timely and effective responses. Transparency is not only a symbol of corporate responsibility, but also a foundation of public trust in a digital society. For victimized customers, information opacity directly affects their ability to prevent personal risks and protect data. If customers do not have timely access to relevant information, it is difficult to take effective action, resulting in greater financial and privacy losses. From the perspective of digital criminology, information transparency is a key element of effective digital regulation. The speed and transparency of a company's response to a data breach is critical to protecting the rights of victims. Lack of information transparency not only weakens corporate compliance, but also affects the health of the digital society as a whole. The requirement for information transparency is not only to make the company take responsibility, but also to reduce the overall impact of data breaches on the public. In the international data protection framework, information transparency has become a key concern for national regulators. For example, the GDPR clearly states that companies must notify affected customers and relevant regulators within 72 hours of a data breach.[1] This strict requirement for information transparency aims to enable customers to understand their situation and take protective measures in the shortest possible time. There are comparative arrangements within the United States, the California Civil Code states that any person or commerce substance that incorporates a data breach must inform the influenced person and certain government organizations.[2] Laws in different regions illustrate that Information transparency is central to worldwide digital regulation. The handling of the Latitude Financial incident highlights the need for Australia to strengthen its regulations and enforcement in this area.

Although OAIC has played a certain role in digital regulation, its regulatory capabilities still have significant limitations. Firstly, OAIC's regulatory measures mainly focus on investigating and punishing incidents after they occur, and there are insufficient preventive measures in advance. OAIC lacks of comprehensive review and risk monitoring capabilities for enterprises. This lack of ability makes it hard for the OAIC to find possible dangers in data management ahead of time. As a result, many data breaches are only handled after serious consequences have already happened. The Latitude Financial occurrence is a typical example. After the hacker effectively invaded and stole a large number of client information, the company did not inform the client at the early of the occurrence, and OAIC's investigation only intervened after the incident occurred, which did not successfully avoid the risk of information breaches. The limitations of post regulatory measures are particularly inadequate in the face of modern digital crimes. With the continuous development of technology, increasingly criminals utilize emerging technologies to hide attack, making data breach detection more difficult.

4.3 Digital Punishment

The punishment in such incidents not only applies to the attacker, but also includes the punishment of the enterprise. For failed to protect customer information, Latitude Financial may experience severe fines and legal action. In the digital society, enterprises bear the heavy responsibility of protecting customer information. Once there is dereliction of duty in data management, they should bear corresponding responsibilities and punishments. latitude financial incident exposed the shortcomings of data protection and risk management, and hackers successfully invaded and stole a large amount of sensitive information. As a restraint measure against businesses that violate their obligations to defend privacy, digital punishment is also used as a response to non-compliance with data breaches. Firms must adhere to high standards of security to avoid data breaches. Enterprises that violate this commitment should bear corresponding legal and economic responsibilities. The purpose of digital punishment is to compensate for the client in the event as well as provide a warning to other businesses. This deterrent effect prompts

[1] European Parliament and Council, Regulation (EU) 2016/679 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation), art 33.

[2] California Civil Code § 1798.82.

companies to invest more tools in data protection, improve personal security methods and risk management mechanisms, thereby reducing the occurrence of future data breaches. By the Australia Privacy Act Amendments passed in 2022, the Privacy Act 1988 was amended and came into effect in 2023. This clause stipulates more severe punishments for serious or repeated violations of privacy and strengthens OAIC's authority to handle data breaches and hold companies accountable for their actions.[1] Other areas, such as the European Union, have comparable regulations in place. GDPR provides provisions for companies to be fined for data protection breaches, up to 4% of the company's global annual revenue or 20 million euros.[2]

However, companies now face civil liability and administrative penalties for data protection vulnerabilities in Australia, but usually do not include criminal liability. Under the provisions of the Privacy Act 1988 and its later amendments, the OAIC may impose large fines for critical or repeated breaches of privacy, but laws in Australia does not directly provide for criminal liability for data protection breaches. Simple civil and administrative liability may not be sufficient to deter data breaches. Although high fines pose a certain deterrent to enterprises, the personal accountability of management is relatively limited. Serious breaches or errors by principal responsible person about data protection that do not contain fraud or harm are often do not need to bear criminal responsibility. This legal framework is difficult to establish sufficient sense of responsibility among individual management when dealing with major data breaches caused by internal negligence within the company. The lack of criminal liability in Australia's data protection laws should be brought up in light of the rise in data breaches and the risk of data privacy vulnerabilities. Especially in the wake of major data breaches quite as Medibank and Latitude Financial in recent years, public and legislative institution should be aware that administrative and civil penalties may not be enough to handle data security threats. The data protection program needs to be made even stronger. This can be done by adding criminal responsibility measures. These measures would ensure that management is held personally responsible in cases of major data breaches. It could also expand the types of individual accountability. In other jurisdictions, for instance, China has formulated the refusal to fulfill information network security management obligations, when a network service provider violates regulations and refusing to right after being ordered by the governmental department to take corrective measures, fines may be imposed on the unit in accordance with the law, and criminal responsibility shall be pursued against its directly responsible supervisors and other directly responsible personnel.[3] These laws may make businesses more responsible in handling customer information and minimize the losses after they occur. This has certain reference significance for Australia.

5. Limitations and Reform Proposals of Digital Criminology

5.1 Conflicts Between Data Privacy Requirements and Regulations

With the rise in digital crimes and the complexity of means, data privacy has become increasingly important, and the dependence on digital evidence is gradually increasing. Businesses and law enforcement organizations must gather, business, and evaluate user data in large quantities during investigations, which poses a danger to personal privacy. Law enforcement may need to look through social media, geolocation records, communications files, and other sources. But large scale data collection not only violates individual privacy rights, but also simply leads to the phenomenon of excessive data collection. Overcollection of data exposes the core contradiction between law enforcement and privacy protection. To deal with complex digital crimes, law enforcement agencies must rely on data analysis, reasonable surveillance and privacy infringement, which could lead to power abuse and even threaten personal freedom. Under strict rules and transparency, boundary issues in data collection and uncontrolled data collection gradually infringe upon specific privacy rights. These are all questions that should be considered. The selection range should be limited to ensure that

[1] Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022.

[2] European Parliament and Council, Regulation (EU) 2016/679 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation), art 83.

[3] Criminal Law of the People's Republic of China (2023 Amendment), art 286-1.

only directly relevant data is collected. This helps to balance the needs of law enforcement with the need to protect privacy. At the same time, a clear system for data reporting should be created. Regularly share information on data collection and usage with the public. An independent oversight institution should be set up to check the data practices of law enforcement agencies. This will help to increase public trust and improve data protection compliance. These steps may improve the relationship between privacy protection and data usage.

5.2 Strengthen Cross-Border Supervision

Coordinating the fight against digital crime on a global scale is challenging because digital crime frequently involves multinational operations. Although the theory of digital criminology can point out the global characteristics of digital crime, further exploration is needed on how to coordinate policies and laws to combat crime on a global scale. The transnational nature of digital crimes and the complexity of technology pose new demands for cross-border cooperation. [1] Due to the fact that the source, target, and transfer of criminal proceeds of cyber attacks may involve multiple countries, so law enforcement agencies from different countries need to collaborate in tracking and responding. This requires countries to establish a cooperative relationship of mutual trust and coordinate in legislation and enforcement procedures. To combat cybercrime, harmonize international legal frameworks, optimize legitimate processes, strengthen cooperation between the public and private sectors, and strike a balance between privacy protection and law responses to tackle evolving digital threats. [2] The existing international mechanisms have significant shortcomings in law enforcement and punishment of transnational crimes, it relies on the judicial systems of various countries makes it difficult to promote law enforcement. Despite convention on Transnational Crime, extradition procedures and legal frameworks frequently prevent successful trials, and some offenders do not get the punishment they deserve. The impact of law enforcement is affected by this complicated transnational crime pattern, which includes various legal procedures for investigations, collection of evidence, extradition, and other such things. [3] The challenges of working together across borders come from differences in each country's legal system. There are also differences in data privacy rules, cyber security practices, and the focus of law enforcement in different nations. Data privacy is protected in the European Union, but some other nations' law enforcement does have broader authority to track criminal suspects.

In addition, political issues often become a major barrier to working together on cross-border digital crime control. This is especially in dealing with hacker attacks that cross borders. The political relationships between the countries involved can directly impact how well and quickly law enforcement agencies can cooperate. The teamwork between Australia and Russia to fight the Medibank data breach has been significantly hampered by the fact that the attackers are from Russia. Substantial sanctions against Russian hackers are difficult to achieve because of the strained relationship between Australia and Russia right now. If Australia imposes more sanctions on Russia, it will make the already tense relationship between the two countries even worse. This will also reduce any possible willingness for the two nations to work together in law enforcement. In the case of Medibank, if the diplomatic situation between Australia and Russia deteriorates more, Australia will be more difficult to ask Russia to provide legal support or extradite the network suspect, which will lead to a vicious circle. Cross-border digital crime cases show how hard it is to coordinate effectively within current international frameworks. This is especially true when handling sensitive national information or political issues. Therefore, it is necessary to rethinking the current global cooperation model, assess its functional effects and practical application, and explore more legally binding and valid cooperation mechanisms. Cross border "mandatory cooperation" clauses can be introduced in this regard, and it is suggested to include "mandatory cooperation" clauses in relevant cybercrime conventions. In specific

[1] Stéphane Leman-Langlois (ed). (2013). *Technocrime, Policing and Surveillance, 71,* Routledge.

[2] Enver Buçaj and Kenan Idrizaj. (2025). The Need for Cybercrime Regulation on a Global Scale by the International Law and Cyber Convention. *Multidisciplinary Review*, *8*, e2025024, 8–9.

[3] Idorenyin Akabom Eyo and Glory Charles Okebugwu. (2024). Analysis of Fundamental Challenges in the Combat of Transnational Crimes. *International Journal of Research and Innovation in Social Science*, 8, 1297, 1305.

major transnational events, countries should provide necessary law enforcement support and data sharing, unless there is a clear national security threat. Without compromising the sovereignty of each country, this would enhance cooperation among countries in transnational digital crime cases.

5.3 Adapt to Technological Update and Strengthen Supervision

The field of digital criminology is always changing as technology develops quickly. This is especially true with the wide use of new technologies like big data and blockchain. Criminal patterns are becoming more complex and varied.[1] The fragmented and private nature of blockchain technology makes it more easily for criminals to carry out illegal transactions and money laundering. However, existing tracking methods are difficult to effectively regulate these anonymous transactions. [2] Digital crime has become more complex as a result of the widespread application of big data evaluation, and criminals gather and analyze significant amounts of user data to carry out detailed fraud or attacks, increasing the success rate. These difficulties highlight the limits of contemporary digital criminology in addressing emerging technologies, that is the existing theories and practices often lag behind technological development and cannot effectively curb crime. To handle the challenges posed by these technology, the field of digital criminology needs to incorporate emerging technologies into its research. Law enforcement agencies should invest in advanced technology for as blockchain monitoring technology to improve their ability to detect hidden acts. Although blockchain technology is used for digital crimes, it can also be used to combat such crimes. The integration of blockchain in investigations provides new tools and methods to address emerging challenges.[3]

6. From Data Breaches to Digital Surveillance

The Latitude Financial data breach not only shows the company's weak data management and the lack of strong regulations, but also raises a deeper question: how harm works in a digital society. In traditional criminology, harm usually means physical injury, property loss, or damage to reputation. But in today's world, where we rely heavily on technology, harm often happens in more hidden, delayed, and long-lasting ways. For example, a person may not notice that their data was stolen at first, but later may suffer from identity theft, financial loss, or emotional stress. This kind of digital harm is not only caused by one person, but often by systems, platform design, company actions, and weak laws working together. More importantly, digital harm is not only found in big companies or public systems. In private life, technology is also used to control and hurt others. For example, in domestic violence, abusers use spy software, smart devices, or cloud accounts to track the victim all the time. This takes away their freedom and causes fear and anxiety. It also shows how new forms of digital abuse are difficult for the law to see or stop. The law often has no clear rules to deal with these kinds of problems. Because of these changes, we need to use theories like digital criminology and surveillance theory to better understand how harm, control, and power now work in a digital world. The next part of this paper will explain these ideas and show how people can become victims even when they are just using normal digital tools in everyday life. It also looks at how laws and rules should change to protect people from these new kinds of harm.

7. Understanding of Digital Criminology Theory

7.1 The Definition of Digital Criminology

In traditional criminology, criminal behavior is usually seen as an individual acting against social rules. It focuses on analyzing the social reasons behind these behaviors and the legal ways to deal with them. However, with the rapid development of digital technology, the forms and meanings of crime are also undergoing significant changes. Digital criminology is an interdisciplinary field that has emerged to address these changes. Digital criminology studies how digital technology affects criminal behavior, the justice system, and society's response. The core of digital criminology is to understand crime in the "digital society." This digital society not only refers to the widespread use of technology, it

[1] Naeem AllahRakha. (2024). Cybercrime and the Legal and Ethical Challenges of Emerging Technologies. *International Journal of Law and Policy*, *2*(5), 28–29.

[2] Shreya Sangal. (2024). Gaurav Duggal and Achint Nigam, 'Blockchain's Double-Edged Sword: Thematic Review of Illegal Activities Using Blockchain. *Journal of Information, Communication and Ethics in Society*, *22*(1), 58, 64–66.

[3] Amit Kumar Tyagi et al. (2024). Role of Blockchain in Digital Forensics. *Role of Blockchain in Digital Forensics*, IGI Global, 208.

also includes how technology deeply affects social relationships, legal systems, and social norms.[1] For example, cyberbullying and online hate speech are not just expressions of personal malice, but also reflect the role of social media platforms in amplifying these behaviors and the helplessness of the law in protecting victims. In the case of Police v Ravshan Usmanov, the defendant acted out of revenge after a breakup, he posted private photos of his ex-girlfriend on Facebook. However, the judge stated that New South Wales lacks clear precedents to hold someone accountable for such crimes. As a result, the defendant was only sentenced to six months in jail.[2] From the perspective of digital criminology, criminal behavior is no longer simply a personal issue. Instead, it is the result of the interaction between technology, society, and law. What must be focused on is, how digital technology has shaped the creation, spread, consequences of criminal behavior and how the law can effectively respond to these changes in this new social context. In addition, digital criminology also requires a re-examination of the boundaries of the law. Traditional law is often based on territorial boundaries, while digital crime has cross-border and cross-space characteristics and this makes existing laws face significant challenges in combating related crimes. These issues need to be considered within a new theoretical framework. Finally, digital criminology not only covers traditional cybercrimes like hacking, identity theft, and cyberbullying, but also involves the impact of digital technology on crime in areas like surveillance, law enforcement, and evidence collection.

7.2 The Importance of "Harm" in the Study of Digital Criminology

The central role of "harm" in the study of digital criminology. In traditional law, "harm" is usually understood as direct damage to a person's body, property, or reputation. However, in the digital society, forms of harm are more diverse and hidden. Compared to traditional physical harm, the harm caused by digital crimes includes not only physical harm to people and property, but also causes emotional harm to the victims. Compared to the limited nature of traditional harm and due to the convenience of information spreading in the digital society, the harm, especially from online defamation, such as damage to the victim's reputation caused by cybercrime can significantly increase the scope and severity of the harm suffered by the victim. In issues related to digital criminology, technology becomes an important medium for causing harm in this process. The emergence of digital technology has changed traditional forms of crime and created new forms of harm. Especially through the spread of digital media and online platforms, the harm has been amplified and prolonged. For example, the online spread of sexual assault images keeps the victim in a state of ongoing trauma, the harm in these digital spaces is endless.[3] And this complex and ever-changing new technology requires a deeper understanding of harm. Digital criminology should rethink the effectiveness of the law in addressing digital harm. Current laws, when dealing with cross-border and highly anonymous digital crimes, it often struggles to hold offenders accountable or protect victims effectively. For example, when personal privacy information is leaked on the internet, even if the victim turns to the law, it is difficult to completely stop or delete the spread of the information. This limitation of legal responses urges us to consider the new risks and challenges brought by technological advancements when making laws and policies. Therefore, the concept of harm becomes especially important in the study of digital criminology.

8. Surveillance Theory

The core of surveillance theory is the use of invisible power to restrain and control individuals. With the advancement of technology, especially the widespread use of information technology, the surveillance capabilities of governments, corporations, and individuals have greatly increased. This not only changed how people interact with each other but also had a deep impact on how surveillance is conducted. In modern society, surveillance has expanded from physical spaces to the digital area. Through data collection and algorithm analysis, control is further achieved. This is not just about how technology extends power and

[1] Anastasia Powell. (2018). *Gregory Stratton and Robin Cameron, Digital Criminology: Crime and Justice in Digital Society*, 3, Routledge.

[2] Police v Ravshan Usmanov [2011] NSWLC 40.

[3] Anastasia Powell. (2018). Gregory Stratton, and Robin Cameron. *Digital Criminology: Crime and Justice in Digital Society*, 97–98, Routledge.

social control,[1] the destruction of privacy and freedom. This technology can not only serve as a tool for crime prevention, it can also serve as a means of social discipline and control. It not only affects individual behavior but also shapes social structures and power relationships.[2] This theory can be specifically reflected in the following characteristics:

First is the characteristic of power and control. Surveillance is not just a way to gather information, it is also a means of exercising power. Through continuous and hidden surveillance, power institutions can effectively monitor people's behavior to achieve the goal of social control. In this news, the domestic violence perpetrator used technological means, like spyware, to exert complete control over the victim, Abigail. Through these surveillance methods, the perpetrator can keep track of her whereabouts, communications, and daily details at any time, they can even interfere with her daily plans, such as deleting her schedule.[3] These technologies allow the perpetrator to dominate both physically and psychologically and through continuous surveillance, they reinforce their power over the victim. This situation shows that, in private relationships, surveillance can also become a powerful tool for control.

Second is the characteristic of concealment. This characteristic is reflected in the effectiveness of surveillance, which comes from its concealment and the uncertainty of those being monitored. Even if people do not know exactly when and where they are being monitored, their behavior will adjust itself out of fear of possibly being observed. This self-discipline does not come from actual surveillance, but from the worry of possibly being monitored at any time. In the news, Abigail mentioned that her mouse moved for no reason and her email account was accessed by someone else. This made her realize that she might be under surveillance. Even though she is not clear about the exact methods and timing of the surveillance, her behavior has already been influenced by the knowledge of being monitored. Especially after the perpetrator learned about her conversations with her therapist, this increased her feelings of anxiety. This uncertainty has caused her behavior to be subject to "self-discipline." She started to stay highly alert in her daily life, constantly worrying about whether she was still being monitored.[4]This fear of surveillance is a reflection of how "invisible power" operates in surveillance theory. Under this characteristic, traditional theories suggest that this practice can deter criminal behavior by increasing the perceived risk of punishment for offenders. However, this view is not entirely accurate. Even under obvious surveillance cameras, professional thieves will still continue to commit crimes. In addition, police officers often engage in serious misconduct even in front of their own vehicle cameras.[5] The "concealment" feature discussed in surveillance theory can also be seen in the Latitude Financial data breach. In this case, the attack was done by external hackers. Their method was highly hidden and indirect. Instead of attacking Latitude's main system directly, they went through a third-party service provider. This way, the company did not notice the attack for a long time. After discovering the problem, the company also delayed telling the public. Many users only learned their information was leaked much later. This delay and lack of communication show a typical type of "invisible harm" in the digital world. The damage does not appear immediately, but becomes serious over time and is often hard to fix. This kind of situation, whether in family relationships or in company data systems, shows how digital crime can be hidden and hard to detect.

The third important characteristic is the diversity of actors. With the widespread use of digital technology, information collection and processing have become much easier. This means that the exercise of power is no longer limited to a single authority. States, businesses, and even individuals can monitor others through technology. This decentralization of power breaks traditional power structures and brings new challenges. In the news report, the

[1] Deborah Lupton. (2015). *Digital Sociology*, 33, Routledge.

[2] M. R. McGuire and Thomas J. Holt (eds). (2017). *The Routledge Handbook of Technology, Crime and Justice*, 21, Routledge.

[3] Grace Atta. (2024). Tech Companies Should Build Products with Domestic Violence Victims in Mind, Expert Says. ABC News. 11 February 2024 https://www.abc.net.au/news/2024-02-11/domestic-violence-perpetrators-misusing-apps-to-cyberstalk/103410954

[4] Atta, above 28.

[5] Stéphane Leman-Langlois. (2013). The Virtual Surveillance Lab: The Creation of a Simulated Experimental Environment. In Stéphane Leman-Langlois (ed), *Technocrime, Policing and Surveillance*, 48-49, Routledge.

perpetrator is described as an ordinary person, they installed surveillance software on common household devices like phones and laptops, gaining access to various private information about the victim.[1] This shows that the misuse of technology is not limited to surveillance at the state level, individuals can also collect information and conduct surveillance using simple technological means. This "diversity of actors" in technology gives ordinary people, and even perpetrators, significant power, this allows them to abuse technology for control in personal relationships. According to a survey by The Office of the Australian Information Commissioner (OAIC), citizens reported that many organizations and businesses collect personal information beyond what is necessary and they feel uneasy about how it is being used. Especially social media platforms and large companies, they believe that these companies excessively collect, store, and share personal data without explicit consent.[2]

Another important characteristic is the normalization and widespread use of surveillance technology. Surveillance is gradually becoming a normal part of society. Whether it is in the workplace, public spaces, or the online world, people are all under different levels of surveillance. This normalized surveillance blurs the boundary between private space and public space. As mentioned in media reports, the technologies used by abusers, such as parental control software and spyware. [3] Although these are legal and common tools in daily life, originally used for family management or safety purposes, when misused, these surveillance technologies have deeply invaded the victim's most private daily life. A report shows that GPS tracking apps and video surveillance devices are widely used, these technologies are used to continuously track and monitor the victims and the use of GPS tracking apps among abusers has increased significantly. Victims are often forced to enable these features, or they will be suspected of improper behavior.[4]

Lastly, there is the digitization of social behavior, this means that with the advancement of surveillance technology, surveillance is no longer limited to physical spaces, actions, communications, transactions, and even emotions can be monitored and analyzed through digital means. This digital surveillance strengthens the full control over social behavior. Abigail's ex-husband not only physically tracked her movements but also interfered with her work and life through digital platforms like email and calendars. [5] This shows that surveillance happens not only in physical spaces but is also everywhere in the virtual world. Abusers use digital methods to gain full control over the victim's life. This behavior shows the application of "digitized social behavior" in surveillance theory. Technology allows the monitoring of people's behavior and information to be seamlessly carried out through the virtual world.

9. Gender and Digital Violence: How Technology Is Used to Control People in Close Relationships

With the wide use of smart devices, social media, and remote control technology, domestic violence has become more connected to technology. This is called "technology-facilitated abuse in family, domestic and sexual violence." These kinds of abuse often use legal or grey-area tools to monitor, follow, control, or harass others. Most victims are women, which shows a clear gender pattern. In the case of Abigail, her ex-husband used spy apps and remote access tools to secretly control her phone, laptop, and email for a long time. He could see her location, daily activities, and even messages about her mental health. This use of technology allowed him to control her even after they were not living together.[6] This kind of behavior is a form of coercive control and is one of the most hidden and underestimated types of domestic violence.

A 2023 report from Australia's eSafety agency says that in many studies and real-life cases, most victims of technology-based abuse are

[1] Atta, above 28.

[2] Office of the Australian Information Commissioner, 'Australian Community Attitudes to Privacy Survey 2020' (Web Page, 2020) https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2020 accessed 5 October 2024.

[3] Atta, above 28.

[4] Delanie Woodlock et al. (2020). *Second National Survey of Technology Abuse and Domestic Violence in Australia* WESNET, 24.

[5] Atta, above 28.

[6] Atta, above 28.

women.[1] Digital forms of intimate partner violence include: forcing someone to share passwords and accounts, checking their messages and calls, using child tracking apps to follow the woman's location, controlling smart home devices to create fear, and sharing or threatening to share private photos or videos. This kind of tech abuse often comes with a pattern called "coercive control." It is not just one event, but part of a cycle of violence. The goal is to take away the victim's freedom, choices, and connection to others. Also, technology-based abuse often happens across many devices and platforms, which makes it harder to stop. On one hand, abusers often know how to use many devices and platforms, so they can control the victim in different ways. On the other hand, social media and online platforms do not respond quickly. It is hard to report abuse, and the steps to give proof are complex. These problems make it harder for victims to get help, and the harm becomes more hidden and more serious over time.

Australia's current laws do not fully deal with this new type of abuse. Although the Criminal code and Privacy act cover some actions like spying, threats, and misuse of information, most court decisions still focus on physical violence and harm that happens right away. It is hard to measure mental harm or digital control that shows up later, and there are no clear legal rules for these cases. Right now, there is a gap between most family violence laws in Australia and new technology. This mismatch is called a "systemic misalignment." Special laws and technical solutions are needed to close this gap. To protect victims of tech abuse, the law should clearly ban the use of spy or tracking software in private relationships. This kind of abuse should be included in the legal definition of family violence. On the platform side, companies should use "safety by design" when building apps. This means showing clear warnings about sharing access, and making it easy to report or block abuse. In the justice system, judges and police need special training to learn how to find and understand tech-based gender abuse and collect the right evidence.

10. The Application of Surveillance Theory in Digital Society and Digital Criminal Justice

10.1 Digital Surveillance and Crime Prevention

In the digital society, surveillance technology is widely used to fight crime. Technologies like video surveillance, data mining, and social media analysis have become important tools in the modern criminal justice system. These technologies can monitor and identify potential threats in real time and improve the efficiency of public safety. Take video surveillance as an example. Over time, CCTV systems have become smaller, more affordable, and more powerful, this is a direct result of technological advancements, meaning that the use and application of CCTV systems are gradually expanding.[2] In the case of Bayley v The Queen, CCTV recorded the last moments of the victim walking on the streets of Melbourne and interacting with Bayley.[3] This is crucial for identifying Bayley as the suspect and speeding up the investigation of the case.

10.2 Cybercrime and Digital Tracking

In digital criminology, surveillance technology is widely used to track and investigate cybercrime activities. By using big data, social media platforms, and communication records, law enforcement agencies can track and investigate criminal activities. This digital tracking increases the crime-solving rate and makes it possible to predict criminal behavior. As pointed out in a study, the investigation of cybercrime is different from traditional crime. The investigation process requires the use of advanced cyber detection technologies, including intrusion detection systems (IDS) to track and detect suspicious activities in real time. It also highlights the importance of online tracking through IP addresses and network accounts. This ensures the ability to quickly locate suspects and take action.[4] But on the other hand, although surveillance technology and digital tracking have improved law enforcement efficiency, it has also brought issues like privacy invasion, risk of wrongful judgments, and misuse. Massive data collection may excessively invade personal privacy. Especially in cybercrime investigations, real-time tracking and data analysis may cause

[1] eSafety Commissioner (Cth). (2023). Technology-Facilitated Abuse in Family, Domestic and Sexual Violence: A Literature Sca.

[2] M. R. McGuire and Thomas J. Holt (eds). (2017). *The Routledge Handbook of Technology, Crime and Justice*, 436, 438, Routledge.

[3] The Queen v Bayley [2013] VSC 313(19 June 2013).

[4] Yanbo Wu et al. (2019). Research on Investigation and Evidence Collection of Cybercrime Cases. *Journal of Physics: Conference Series*, *1176*, 042064, 3-4.

improper interference with innocent people. Moreover, reliance on technology may lead law enforcement agencies to depend too much on algorithms and neglect the strict verification of evidence, this creates the risk of unfair law enforcement.

10.3 Personal Privacy and Technology Misuse

As surveillance technology becomes more widespread, personal privacy faces increasing threats. For example, in domestic violence cases, abusers use legal surveillance technology to track and control victims, they even continue to digitally monitor them after the divorce. This phenomenon highlights the violation of personal privacy and security when surveillance technology is misused. A survey shows that, potential offenders can easily access various technological tools through search engines like Google, these tools include surveillance apps, spyware, GPS tracking devices, and more. The search engine's predictive feature will recommend similar queries based on the user's search habits and popular search trends. This suggests that when potential abusers conduct similar searches, they are likely to come across suggestions or tools related to technology misuse, further increasing their ability to carry out tech-based abuse.[1] Therefore, it becomes very necessary to limit this kind of behavior, strengthening legal regulation is needed. Limit the misuse of technology and provide more protection measures for victims, such as safe technology education. And require search engines to optimize algorithms to avoid recommending abusive tools, while pushing tech companies to enhance their reviews for illegal usage.

10.4 The Risks and Ethical Reflections of Digital Surveillance

Although digital surveillance technology helps prevent crime and improve public safety, its misuse also brings serious ethical risks and problems for society.

First, too much surveillance can take away personal freedom. When people know they might be watched at any time, they often change how they speak and act. They may not feel safe to express their true thoughts. Even if no one is forcing them, this kind of unclear situation can make people feel nervous for a long time and affect their privacy and mental health. Second, we cannot ignore problems like algorithm bias and data discrimination. Many digital surveillance systems use artificial intelligence and big data, but these systems are often trained with unbalanced data. Because of this, they may not work the same for everyone. For example, a study by Buolamwini and Gebru showed that many gender recognition systems are much more accurate for male faces than for female faces. This kind of unfair result makes the system less trustworthy and may harm people from minority groups.[2]

Also, there are no clear rules about how long personal data can be kept, who can see it, or how people can delete it. When people do not have control over their own data, it can lead to mistrust and misuse. To solve this, the government and other organizations should make better laws to clearly say how surveillance data can be used and where the limits are. Independent groups should check the use of this technology regularly. Only by protecting both safety and personal privacy can we build a fair and sustainable digital society.

11. Conclusion

As digital society keeps growing, traditional ideas about harm, control, and responsibility are being challenged. This paper looked at the Latitude Financial data breach and tech abuse in close relationships. It showed that digital harm is often hidden, happens later, and comes from many causes working together. These include poor company decisions, bad platform design, and weak law enforcement. Because digital crimes often involve high technology, cross-border actions, and hidden identities, they are hard to stop and hard to punish under old legal systems. Digital criminology and surveillance theory help us better understand these new problems. These theories show that power today often comes from technology, not just from people or rules. They also teach us that harm is not always physical—it can be emotional or social, caused by digital tools. The law must change to deal with this. In the future, privacy laws, criminal laws, and domestic violence laws should include rules about technology misuse. Tech companies should design safer apps, and the idea of "safety by

[1] Lisa Sugiura et al. (2024). The Technification of Domestic Abuse: Methods, Tools and Criminal Justice Responses. *Criminology & Criminal Justice*, 1, 6–8.

[2] Joy Buolamwini and Timnit Gebru. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research, 81*, 1, 8.

design" should be required. Countries must also work together better to stop global digital crimes. Legal research should go beyond old ideas. It should pay more attention to how fast technology changes and how it affects people. Only when law, technology, and ethics work together can we really protect people in the digital world and build a fair and safe digital society.

References

ABC News. (2023). Latitude Financial Customers Frustrated by Lack of Communication after Cyberattack. 28 March 2023 https://www.abc.net.au/news/2023-03-28/latitude-financial-customers-frustrated-lack-of-communication/102151166 accessed 12 October 2024.

Abraham D. Sofaer and Seymour E. Goodman. (2001). *Cyber Crime and Security: The Transnational Dimension.* Hoover Institution Press.

Amit Kumar Tyagi et al. (2024). Role of Blockchain in Digital Forensics. *Role of Blockchain in Digital Forensics* (IGI Global).

Anastasia Powell. (2018). Gregory Stratton and Robin Cameron, *Digital Criminology: Crime and Justice in Digital Societ,* Routledge.

California Civil Code

Criminal Law of the People's Republic of China (2023 Amendment)

Deborah Lupton. (2015). *Digital Sociology.* Routledge.

Delanie Woodlock et al. (2020). *Second National Survey of Technology Abuse and Domestic Violence in Australia*. WESNET.

Enver Buçaj and Kenan Idrizaj. (2025). The Need for Cybercrime Regulation on a Global Scale by the International Law and Cyber Convention. *Multidisciplinary Review, 8*, e2025024.

eSafety Commissioner (Cth). (2023). *Technology-Facilitated Abuse in Family, Domestic and Sexual Violence: A Literature Scan*.

European Parliament and Council. (2016). Regulation (EU) 2016/679 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation).

Gavin J D Smith, Lyria Bennett Moses and Janet Chan. (2017). The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-Driven Approach. *British Journal of Criminology,* 57, 259.

Grace Atta. (2024). Tech Companies Should Build Products with Domestic Violence Victims in Mind, Expert Says. ABC News, 11 February 2024. https://www.abc.net.au/news/2024-02-11/domestic-violence-perpetrators-misusing-apps-to-cyberstalk/103410954

Idorenyin Akabom Eyo and Glory Charles Okebugwu. (2024). Analysis of Fundamental Challenges in the Combat of Transnational Crimes. *International Journal of Research and Innovation in Social Science, 8*, 1297.

Joy Buolamwini and Timnit Gebru. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research*, *81*, 1.

Lisa Sugiura et al. (2024). The Technification of Domestic Abuse: Methods, Tools and Criminal Justice Responses. *Criminology & Criminal Justice, 1*.

Maria Fernanda Pires. (2024). AI and Machine Learning: Revolutionizing Supply Chain Security. *Advances in Computer Sciences*, 7, 1.

Mariya Ouaissa et al (eds). (2022). *Big Data Analytics and Computational Intelligence for Cybersecurity.* Springer.

Md Abu Imran Mallick and Rishab Nath. (2024). Navigating the Cybersecurity Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. *World Scientific News, 190*(1) 1.

Naeem AllahRakha. (2024). Cybercrime and the Legal and Ethical Challenges of Emerging Technologies. *International Journal of Law and Policy, 2*(5), 28.

Naeem AllahRakha. (2024). Transformation of Crimes (Cybercrimes) in Digital Age. *International Journal of Law and Policy*, 2(2), 1, 8.

Office of the Australian Information Commissioner. (2020). Australian Community Attitudes to Privacy Survey 2020.

https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2020 accessed 5 October 2024.

Office of the Australian Information Commissioner. (January 2014). *Australian Privacy Principles*, APP 11.

Police v Ravshan Usmanov [2011] NSWLC 40

Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022

M. R. McGuire and Thomas J. Holt (eds). (2017). *The Routledge Handbook of Technology, Crime and Justice,* Routledge.

Shreya Sangal, Gaurav Duggal and Achint Nigam. (2024). Blockchain's Double-Edged Sword: Thematic Review of Illegal Activities Using Blockchain. *Journal of Information, Communication and Ethics in Society*, *22*(1), 58.

Stéphane Leman-Langlois (ed), (2013). *Technocrime, Policing and Surveillance, 71,* Routledge.

Stéphane Leman-Langlois. (2013). The Virtual Surveillance Lab: The Creation of a Simulated Experimental Environment. In Stéphane Leman-Langlois (ed), *Technocrime, Policing and Surveillance.* Routledge.

Stephen Smiley. (2017). Equifax: Australians' Sensitive Financial Information at Risk in Data Breach of US Company. *ABC News* (online, 8 September 2017) https://www.abc.net.au/news/2017-09-08/smiley-credit-check-australians-financial-information-at-risk/8887198.

The Queen v Bayley [2013] VSC 313(19 June 2013)

Yanbo Wu et al. (2019). Research on Investigation and Evidence Collection of Cybercrime Cases. *Journal of Physics: Conference Serie*s, 1176, 042064.