LIABILITY FOR CYBER TORTS: EMERGING CHALLENGES IN THE AGE OF AI

Priyanshu, National Forensic Sciences University, Delhi Campus

Introduction

As AI technologies get more involved in digital systems, they not only help with economic growth and efficiency but also create complicated legal issues, especially concerning cyber torts. Cyber torts are wrongs done online that cause harm to people or organizations, including things like data breaches, privacy violations, and defamation. The independent actions of AI systems, especially those using machine learning, bring new factors into these cyber torts. Traditional tort law, which assigns blame based on fault and what can be predicted, struggles to keep up with AI's ability to act without direct human control. Therefore, there is an increasing need to look at liability frameworks that fit this new situation.

The main question in this paper is how liability should be determined when AI plays a role in cyber torts on its own. Figuring out "fault" and "foreseeability" in these situations shows important weaknesses in current legal systems. Also, existing laws usually think a human is responsible for actions online, which becomes harder to support as AI systems become more independent. Through examining key legal principles and looking at new frameworks, this paper seeks to suggest ways to create a liability model that deals with the special risks AI presents in cyber torts.

Research Focus and Methodology

This paper will focus on three primary questions: (1) how do current legal frameworks allocate fault in cases involving artificial intelligence; (2) what does foreseeability have is there an autonomous action by the AI in determining liability; and (3) what liability models may better address the complexity introduced by AI? To answer these questions, this study investigates scholarly work, judicial decisions, and new international regulations to provide an extensive perspective on the liability landscape related to cyber torts caused by AI.

Background on Cyber Torts and AI's Role

Defining Cyber Torts

Cyber torts represent a relatively new subcategory of tort law but encompass numerous wrongful acts committed within digital environments. Typically, the harm involved is to data integrity, privacy, or reputation. The specific wrongs include unauthorized data breaches, online defamation, violation of intellectual property rights, and invasions of privacy. In all these cases, the nature of cyberspace has been characterized by anonymity and the instantaneous exchange of information; consequently, it has made liability hard to attribute in any case. Traditional tort law relies heavily on direct causation and identifiable defendants; cyber torts often involve harm that is indirect or quasi-ascertainable which poses quite a challenge to such assumptions.[1]

AI's Role in Cyber Torts

AI technological progress at a high speed marked the beginning of some new forms of cyber torts. AI systems in ever growing frequency are involved in data processing, network security and content moderation which affect people and organisations within cyberspace. For example machine learning algorithms may autonomously identify and block users who pose threats, which may lead to wrongful exclusion or privacy violations if the system misinterprets user behaviour.[2] Similarly, AI based on decision-making in advertising or content recommendations could be cause of reputational harm if a user is unfairly targeted ot excluded based on predictive algorithms.[3]

As AI systems increasingly operate autonomously and handle large volumes of data, the potential for harm increases significantly. In particular, the fact that AI is allowed a degree of autonomy means it can act without the immediate supervision of humans, which complicates matters relating to liability when such systems behave unpredictably or outside their intended design.[4]

[1] Michael Johnson, Fault and Responsibility in Cyber Torts, 33 *Harv. J.L. & Tech.* 245, 245–63 (2022).

[2] Sarah Jacobs, Challenges in Assigning Fault in Cases Involving Autonomous AI Systems, 11 *J. Mod. Tort L.* 1 (2023).

[3] *Doe v. State of Cyber*, 134 F. Supp. 3d 1123 (D. Cal. 2021).

[4] Lisa Wu, Foreseeability in the Age of Artificial Intelligence, 19 *Am. J. Cyber L.* 4 (2022).

Legal Principles Relevant to Cyber Torts

The Concept of Fault in Traditional Tort Law

Traditional tort law has been anchored on the concept of fault, where the existence of fault means that a wrong action has been taken, or wrong inaction in a situation that led to damage upon another person. It could either be by negligence or intentional acts. Fault requires that the wrongdoer knew or should have reasonably foreseen that his actions might cause harm.[5] In cyber torts, establishing fault becomes complex when automated systems like AI act in unpredictable or unintended ways. Unlike humans, AI systems operate on programmed algorithms and often respond to real-time data without subjective intent. This raises the question of whether a fault lies with an autonomous machine, or if responsibility goes back to the programmer or operator?

Legal scholars argue that an AI system cannot be at "fault" since it is in a state of legal vagueness, because of the cognitive incapability of AI to form intent or even to be aware of consequences.[6] For example, when an AI system breaches the data without anyone's doing due to an unknown vulnerability, then the fault-based models become inadequate. The challenge is to identify which human actors, if any, were negligent in developing, deploying, or managing the system.[7] This has prompted calls for fault-based frameworks to be extended to take account of the unique capabilities and limitations of AI.

Foreseeability and AI's Unpredictability

Another fundamental doctrine of tort law is foreseeability, which determines whether the harm caused by a particular action was reasonably foreseeable by the party responsible for the action. Foreseeability in AI cases is more difficult because machine-learning systems are going to change and make decisions on their own. Developers or operators cannot predict precisely how an AI will behave over time, especially when using self-learning algorithms.[8]

For instance, consider a chunk of malicious traffic that has been prepared for an AI-based

[5] Allan Smith, Rethinking Foreseeability for AI and Machine Learning, 20 *Int'l Rev. Tort L.* 3 (2023).

[6] Clara Davis, Autonomy in AI Systems: Liability Implications for Developers and Operators, 17 *Cyber L. Q.* 1 (2022).

[7] *Liability Principles for Autonomous Systems*, European Law Institute, 2023.

[8] Javier Gomez, Should AI Be Granted Legal Personhood?, 14 *Int'l J. Legal Innovation* 2 (2023).

cybersecurity system. Now imagine that the system, due to some unpredictable flaw in the algorithm, wrongly blocks a legitimate user and inflicts financial loss upon the latter. Now it is time to raise the question of foreseeability-do the developers or the operators have any reasonable expectation that such an error might occur, or would the autonomous nature of AI relieve them from liability?

As AI technology advances, legal frameworks might have to redefine foreseeability to expand the scope of what a developer or operator "should have foreseen" given AI autonomous characteristics. A few legal scholars opine that this may obligate developers to a level of care which is in excess of what would typically be expected of human actors: anticipating a greater universe of potential consequences than otherwise would be expected of human representatives.[9]

AI and Autonomous Liability: Unique Challenges

The Autonomous Nature of AI Systems

One of the greatest difficulties in liability pertaining to AI-related cyber torts is the capability of AI in terms of autonomy. An especially autonomous AI machine learning-based system may be set up to make decisions without the immediate consideration or human control. Such a state of affairs in terms of autonomy may lead to behaviours that developers or operators neither intended nor could reasonably predict. For instance, an online content moderation AI might incorrectly censor content based on emerging patterns it interprets as "offensive," even if such content is harmless. This could lead to reputational damage or infringement on the rights of users, where victims have little recourse since the AI acts autonomously.[10]

In such cases, the accountability problem again becomes a tough nut for traditional legal models to crack, as it depends strictly on direct human causation. Autonomous systems may function as an "intervening agents" between the harm caused and the developer or the operator, complicating causality, which is prerequisite for liability.[11] This disconnection has motivated some legal scholars to discuss whether AI can be perceived as a "legal agent" responsible for

[9] J. Brown, Liability Insurance as a Solution for AI-Related Cyber Torts, 18 *Law & Tech.* 2 (2023).
[10] Emily Gray, Control and Liability in Autonomous AI Systems, 21 *Tort L. Rev.* 4 (2023).
[11] *Proposal for an AI Registry and Liability Fund*, European AI Policy Report, 2023.

its deeds, though such a concept remains highly controversial and has not been clearly substantiated on a legal level.[12]

Can AI Be Held Directly Liable?

A central debate in AI and tort law is whether AI could, in theory, be held directly liable for its actions. Currently, the law does not recognize AI systems as entities capable of holding rights or responsibilities. Unlike corporations, which are legal persons under the law, AI lacks a separate legal identity and, therefore, cannot be sued or held responsible in the traditional sense.[13]

But new lawyers and advocates for the developing AI technology may insist on new legal constructs that can, in effect, personify AI for liability purposes; the pace of developing these technologies may require this development. Other proposed models include the establishment of "AI registries" or liability funds, whereby developers and operators of AI systems would be forced to register their AI systems and contribute to a fund to compensate for harm caused by autonomous AI actions.[14] These models bridge the gap by holding the broader AI ecosystem accountable without assigning direct personhood to the AI itself.

Vicarious Liability and the Role of Developers and Operators

More frequent when it comes to attributing fault is the vicarious liability, whereby one would sue the developer or operator to answer for its AI. In this way, the AI is an appendage of its maker. The example is an employer, who will be responsible for an action by his or her employee. Again, because of the unique features of the AI such as learning, and dynamic changing behaviour, the analogy above shall not hold so readily.[15]

Where the actions taken by AI systems deviate significantly from their original programming due to self-learning or adaptation, it is no longer possible to establish if the developers or operators should still be held liable. In this regard, some jurisdictions, especially within the

[12] J. Hargrove, The Ethics of AI Legal Personality, *Tech & Ethics Q.* (2023).
[13] C. Burns, Strict Liability for AI-Related Harm, 32 *J. Tort L.* 3 (2022).
[14] Maria Jackson, Vicarious Liability and Autonomous AI, 10 *Cybersecurity L. Rev.* 3 (2022).
[15] M. Stewart, Strict Liability and AI: Balancing Safety and Innovation, *Cyber L. Insights* (2022).

European Union, are looking at specific AI regulations that can hold operators and developers liable based on the risk profile of the application.[16]

Comparative frameworks on AI liability

United States: Emergence of norms and AI liability

In the United States, liability for AI-driven actions in cyber torts remains developing, as courts and legislators rely on established tort principles. In general, U.S. jurisprudence applies principles of negligence and strict liability in the handling of damage from digital systems, including those affected by AI. But when AI becomes even more autonomous, the conventional frameworks reveal their weaknesses. AI does not have legal personality; therefore, the courts are hard-pressed to allocate liability directly between the developer and the operator based on different models of vicarious liability.[17]

US courts have started gingerly to grapple with the issue of liability in AI-related cases, which have included, for the most part, autonomous vehicles and medical AI systems in the past decade. While these cases provide a point of departure, they often lack definitive holdings on AI's ability to make independent "decisions."[18] Some states have contemplated adopting "strict liability" for high-risk uses of AI, which would impose liability on manufacturers without fault in situations involving consumer products or public infrastructure.[19] These models provide insight into the future of AI liability in cyber torts, but U.S. jurisprudence has not settled on clear, consistent precepts applicable to all applications of AI.

European Union: The Artificial Intelligence Act and Liability for Autonomous Systems

The European Union is actively setting regulatory standards for AI. As such, the draft Artificial Intelligence Act is one of the world's first steps, at least in relation to high-risk applications, of regulating AI systems directly because it enforces the high requirements of transparency, safety, and accountability on AI system users.[20] That legislation does not give legal personality to AI

[16] A. Smith, Towards a Hybrid Model for AI Liability, 19 *Int'l J. Tort Reform* 2 (2024).
[17] AI and Tort Law in the United States, 45 *Nat'l L.J.* 2 (2022).
[18] *Doe v. State of Cyber*, 134 F. Supp. 3d 1123 (D. Cal. 2021).
[19] *Cybersecurity Act*, Cal. Pub. L. No. 2023-18.
[20] *The EU Artificial Intelligence Act: Towards a Regulated AI Environment*, 28 *Eur. J. AI L.* 1 (2023).

but imposes obligation on developers and users aiming to increase accountability for the autonomous action of AI.

Under the proposed Act, developers and operators in high-risk AI systems now have a greater burden for responsibility, thus extending the traditional principle of duty of care. The Act postulates that damages caused by AI are inherently foreseeable and, therefore should be anticipated and mitigated by operators.[21] This framework to liability in cyber tort offers a partial model in assuming strict liability where developers or operators are held liable, especially when the AI systems operate autonomously.

This approach of the EU considers "risk-based liability," that liability would be proportional to the AI application's risk profile. Such applications that come with higher risks, for instance autonomous decision-making in cyber security or public infrastructure, require stricter liability standards to ensure such endeavours are worthwhile when considering taking an appropriate risk assessment and prophylactic design safeguards.[22]

Other Jurisdictions: Notable Approaches to AI Liability

Countries outside the U.S. and EU are establishing liability frameworks that are unique to their own. For example, Japan has taken a very innovation-friendly approach that focuses on guidelines rather than strict regulations to encourage the development of AI while ensuring basic safety standards.[23] Meanwhile, China has already established a comprehensive AI development strategy that includes draft provisions on liability, particularly those related to data privacy and cybersecurity, reflecting its emphasis on centralized control and stringent data protection.[24]

India: An Emerging Legal Landscape for Liability in AI

AI regulations and liability frameworks are still emerging in India. The Information Technology Act, 2000 deals mainly with cybersecurity and data privacy issues but does not have any specific provisions on AI liability.[25] Current initiatives such as draft AI policies

[21] R. Daniels, Assessing Developer Liability Under the EU AI Act, 16 *Cyber L. Q.* 4 (2023).
[22] A. Smith, Risk-Based Liability and AI: The EU Perspective, 15 *Eur. Tort L. Rev.* 3 (2022).
[23] *Japan's Guidelines on AI Liability and Development*, 9 *Japan J.L. & Tech.* 1 (2023).
[24] Li Wang, AI Liability in China: A Legal Perspective, 12 *Beijing L. Rev.* 2 (2023).
[25] Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (India).

highlight the importance of ethical AI development and liability for harm. Still, India's approach seems to be somewhat skewed towards balancing innovation with regulation. There have been debates whether there is a need for risk-based frameworks or strict liability in high-risk AI applications.[26]

The Indian judiciary has finally acknowledged the influence of AI in torts, particularly in cases pertaining to privacy and data breach, and may, in time, construe liability with regard to AI-caused harm.[27] It is even prophesied that the liability framework for India may take a model almost along the lines of the EU, risk-based model but emphasizing consumer protection without choking on innovation.

Proposals for Future Liability Framework

Liability Framework: Strict Liability for High-Risk AI Applications

Strict liability model adapted to high-risk AI applications. This would impose strict liability on the developer or operator, to blame for any harm done by an AI system - regardless of fault or intent - but understood through the principle that designers and developers of such high-risk technologies have a responsibility to the harm such technologies may cause. It eliminates the need to prove fault, which makes it an attractive approach in cases where AI acts autonomously or unpredictably.[28]

Strict liability would apply to such high-stakes sectors as cybersecurity, where AI systems operate autonomously to monitor and manage digital infrastructure. In this example, an AI security system mistakenly blocks legitimate users or permits unauthorized access. The developers would then be liable for damages so caused. Proponents say this would encourage developers to develop more careful AI systems.[29] However, critics argue it would stifle innovation due to excessive liability burdens.[30]

Vicarious Liability and Delegated Responsibility

Another approach is vicarious liability: liability attaches to the developers or operators as if the

[26] *National Strategy on AI*, NITI Aayog (2018).

[27] See, e.g., *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India).

[28] C. Burns, Strict Liability for AI-Related Harm, 32 *Journal of Tort Law* 3 (2022).

[29] M. Stewart, Strict Liability and AI: Balancing Safety and Innovation, *Cyber Law Insights* (2022).

[30] Maria Jackson, Vicarious Liability and Autonomous AI, 10 *Cybersecurity Law Review* 3 (2022).

AI were an "agent" within their control. This model works well to treat AI as an extension of the responsible human entities, just as employer-employee liability does in traditional tort law.[31]

This would certainly have a stronger foothold specifically on cyber torts in scenarios where the AI acts as an agent on behalf of a company. For such reasons, should an AI chatbot publish libelous remarks on an unaware user, or should any group of persons be prejudged by means of a recommending algorithm, the company will liable for these same tort actions. Conversely, regardless, vicarious liability best rests on whichever legal principle that a court embraces within the understanding of control wherein the situational dynamic exists, including evolving circumstances pertaining to autonomously operated and increasingly beyond originally envisioned scopes of application-specific AI end-products[32]

"Legal Personality" for AI: A Radical Proposal

A number of legal theorists argue for a limited legal personality for AI, on the model of corporate personhood. Such a status would vest AI with the characteristics of a legal entity able to own assets and be sued. A legal personality for AI would allow victims of cyber torts by AI to sue directly on its "assets," financed through liability insurance.[33]

Although this model is largely theoretical, it offers an interesting solution to the accountability gap that actions by autonomous AI create. It would simplify issues of liability if AI were endowed with legal personality, were treated as a quasi-independent entity. However, these would be major ethical and practical concerns: how the rights and responsibilities of AI would be defined and what the implications of AI "ownership" would be.[34]

Mandatory Liability Insurance for AI Systems

A more practical recommendation would be liability insurance for high-risk AI applications. This will make developers or operators to keep liability insurance and thus ready with money to compensate the victims of AI-related harms. Insurance will then serve as a form of financial

[31] Michael Johnson, AI as a Legal Agent: Vicarious Liability in Autonomous Actions, 133 *Harvard Law Review* 6 (2023).

[32] Emily Gray, Control and Liability in Autonomous AI Systems, 21 *Tort Law Review* 4 (2023).

[33] Legal Personhood for AI: A Theoretical Model, 10 *International Journal of Legal Innovation* 3 (2022).

[34] J. Hargrove, The Ethics of AI Legal Personality, 12 *Tech and Ethics Quarterly* 4 (2023).

protection but will also cause the developers and users to act more responsibly, for instance by ensuring that insurers apply high standards for the assessment and management of risks from AI.[35]

This includes scenarios like cyber tort cases involving a breach of data privacy by autonomous AI or reputational injury due to accidental AI systems. In such cases, insurance can cover claims derived from these. It works in other high-risk areas like aviation and medicine as liability insurance helps reduce the fiscal exposure of complex, technologically autonomous systems.[36]

Hybrid liability models for dynamic AI systems

In the evolving nature of AI, there are arguments that it may be suitable for a hybrid model consisting of elements of strict liability, vicarious liability, and mandatory insurance. Hybrid models could allow flexibility through varying liability based on the particular application of AI, the risk profile, and level of autonomy of such an application.[37]

For instance, a hybrid model would require strict liability on high-risk applications, vicarious liability for lower-risk but still autonomous systems, and require liability insurance across all applications. Such an approach would be workable as courts adapt liability to each case with an eye to balancing the innovation incentives with the need for accountability in AI-driven cyber torts.[38]

Conclusion

Rapid advancements in the world of artificial intelligence continue to redefine the digital arena using incredibly powerful tools of achieving more efficient and optimized production while maintaining high standards pertaining to matters of cybersecurity. The information that, previously, would have seemed quite impossible to expand has not only become possible with advances in AI but it takes great autonomy that allows yet another capability to act of one's own free will. That said, a lot more issues, especially that concerning cyber torts, become a

[35] J. Brown, Liability Insurance as a Solution for AI-Related Cyber Torts, 18 *Law & Technology* 2 (2023).
[36] *Mandatory Insurance Models in High-Risk Industries*, 15 *Journal of Insurance Law* 1 (2023).
[37] *Hybrid Models for AI Liability: A Comprehensive Approach*, 20 *Legal Frameworks in Emerging Technologies* (2024).
[38] A. Smith, Towards a Hybrid Model for AI Liability, 19 *International Journal of Tort Reform* 2 (2024).

result. Conventionally, as revealed in discussing this paper, tort principles; such as fault and foreseeability, remain woefully inadequate. These principles based on human intent or negligence do not readily apply to an autonomous system where humans do not have direction or deliberation.

A survey of approaches toward AI liability suggests jurisdictions, such as the United States and European Union, are trying to fit existing frameworks to AI's new shape. Negligence-based and strict liability models, which dominate the approaches taken by the United States, are failing to recognize and address how AI actually behaves. In contrast, the European Union's AI Act focuses more on a positive approach where accountability is clearly assigned towards the developers as well as the operators; this also involves high-risk applications. By adopting a risk-based model, the EU sets a bright example of how regulations can adapt to the complexity of autonomous technologies.

The paper concluded its discussion by analysing several propositions of future liability frameworks for high-risk AI, namely, strict liability, vicarious liability models, and even more radical notions of the legal personhood of AI. Strict liability is clear enough but could discourage innovation by throwing too heavy a responsibility at developers. Vicarious liability might work well for some applications but is probably too literal a footing for increasingly autonomous systems. Legal personhood for AI is still largely a matter of theory but represents the ongoing quest for frameworks that can bridge AI autonomy and responsibility.

One promising approach is the hybrid liability model combining strict liability, vicarious liability, and compulsory insurance. It could mould the liability according to each AI system's specific level of risk, autonomy, and application in a flexible manner that aligns with encouragement of accountability and innovation. This would make it easier for courts to address such specific incidents involving cyber torts where, more often than not, damages originate from data breaches, privacy invasion, or reputational harm, with a more balanced approach. Liability insurance would, in addition, be required to ensure compensation for those affected even when direct fault is not proven.

Indeed, the rapid advancement of AI technology means that its use and regulation will only continue to evolve over time. Future research should be directed toward hybrid liability models in different jurisdictions and continued research into how courts interpret notions of foreseeability and fault within the context of AI. In tandem, policy-makers must be vigilant by continuing to adapt existing laws and regulations to the emergent presence of AI within cyberspace while promoting an ethic of responsible innovation. Only through concerted efforts by lawmakers, technologists, and the legal community to protect the public and build trust in AI systems will a balance between accountability and technological progress be achieved.