techellect™ AI & IQ working together

cyberconIQ

Who's Liable When AI Acts on Its Own?

By Dr. James L. Norrie, DPM, LL.M | September 24, 2025

Abstract

Agentic AI is no longer a futuristic abstraction. And these systems do not simply respond to human commands; they can take action on your behalf as individuals or organizations. They can negotiate, schedule, trade, purchase, all while making judgments that ripple into legal and financial consequences for you. In that moment, they are not just collaborative tools anymore, they are your authorized agent. And once you cross that threshold, an urgent question arises: when your AI acts, who is liable?

Common law has always traditionally assumed a human actor at the center of legal accountability. Intent, consent, and knowledge are its cornerstones. We punish negligence, fraud, or malice precisely because we can assign them to a person acting with intent. But what happens when an AI system takes an action that you did not foresee and perhaps cannot even fully understand? If you gave the instructions in broad terms, did you consent to the outcome? If the system acted autonomously, where is the human intent? Can you claim ignorance of what AI might do and use that as a defense? These are no longer abstract hypotheticals but the urgent dilemmas beginning to confront regulators, courts, and companies today.

The European Union's AI Act, passed in 2024, at least begins to grapple with this reality. It creates a framework for classifying and constraining high-risk AI. More tellingly, the EU has updated its Product Liability Directive, extending strict liability to software, including AI, ensuring that developers can be held responsible for harms caused even when fault cannot be proven. The proposed AI Liability Directive goes further, making it easier for victims to pursue claims. Regulators such as ESMA have already made clear that banks cannot hide behind opaque algorithms, insisting executives remain responsible when AI is used in financial decision-making.

Across the Atlantic, the U.S. remains mired in patchwork approaches and half-measures. Some policymakers flirt with bold proposals, like binding pre-deployment safety testing, while others attempt to freeze state-level regulation for a decade, effectively handing Big Tech a free pass at the very moment accountability is most needed. Industry lawyers now write primers on indemnities and insurance for agentic AI, while scholars propose "law-following AI" that refuses unlawful commands even from its human masters. Yet amid this swirl of activity, one uncomfortable truth persists: without clear rules, responsibility will disperse into what some call *moral crumple zones*, spaces where blame is absorbed and diffused until no one is accountable.

Big Tech knows this. Indeed, it is their preferred terrain, one where legal liability evaporates in the fog of algorithmic ambiguity. The question is whether we will let them succeed in designing systems of power without designing systems of responsibility.

The stakes are not limited to corporate boardrooms or courtrooms. If harms caused by agentic AI cannot be traced back to a responsible party, public trust will wither. Victims will be left without remedy. Worse, we may see a replay of the early internet, when platforms insisted they were neutral conduits and thus exempt from responsibility, a claim that delayed meaningful accountability for years and left societies grappling with disinformation, online harms, and unchecked digital monopolies. To repeat that mistake with agentic AI would be catastrophic, because this time the machines do not merely mediate speech, they act directly in the world.

This suggests the responsibility cannot rest solely with lawmakers or regulators, although their role is urgent and undeniable. Instead, responsibility to act extends to each of us. The rise of agentic AI is not only a technical and legal frontier, it is a moral one. To ignore the implications, to delegate our choices to machines without demanding accountability, is to quietly concede that justice itself may become optional.

Which brings me to you, the reader. If you have read this far, you already sense that something profound is at stake. The question is, what will you do? Will you demand that companies disclose how their AI makes decisions? Will you support policymakers who insist on transparency and liability rather than deferral and delay? Will you question whether delegating more of your own choices to machines erodes not only your agency but also your responsibility?

Your personal action plan need not be grand. It can begin with insisting that the AI tools you use respect privacy, fairness, and transparency. It can include pushing your employer to adopt standards that put human oversight above automation. And it can grow into advocacy for laws that treat AI not as a black box but as a mirror of human choices, bound to the same expectations of accountability and justice.

The promise of agentic AI is immense, but so too is its peril. The law always struggles to catch up by its very nature of looking at past cases for guidance on future conduct. So, regulators will argue, corporations will lobby, and courts will hesitate. Meanwhile, Big Tech will press forward, happy to operate in the moral crumple zones where no one bears responsibility. The question is whether you, and we, will let them.

Author Bio:
Dr. James L. Norrie is a professor of Law and Cybersecurity, and Founding Dean of the Graham School of Business, at York College of Pennsylvania (http://www.ycp.edu). He wrote *Beyond the Code: AI's Promise, Peril and Possibility for Humanity* (KH, 2025).

Learn more about our free community of interest in ethical AI at: www.techellect.com or visit www.cyberconIQ.com to discover innovative AI security tools. To purchase his book, click on the QR code, or visit: https://he.kendallhunt.com/product/beyond-code-ais-promise-peril-and-possibility-humanity