

Intellectual Property & Technology Law Journal

Edited by the Technology and Proprietary Rights Group of Weil, Gotshal & Manges LLP

VOLUME 38 • NUMBER 10 • NOVEMBER-DECEMBER 2026

Distributed Digital Liability: Understanding Accountability in Disaggregated Digital Operations

By Steven W. Teppler

Modern digital operations are dynamic by design. Organizations continually reconfigure their operations as they adopt new technologies, new service models, and new operational relationships. Importantly, however, few (and increasingly fewer) enterprises today own, manage, or directly control every component of the operational environments upon which they depend. Cloud computing, software-as-a-service, managed service providers, managed security service providers, software supply chains, federated identity platforms, artificial intelligence, and increasingly specialized technology vendors have transformed not simply the tools organizations use, but the manner in which digital operations themselves are conducted.¹

These developments reflect neither accident nor experimentation. They are the product of rational business decisions intended to improve efficiency, resilience, scalability, innovation, and access to expertise. Individually, each decision appears discrete. Collectively, however, they have quietly reshaped the operational architecture through which modern organizations conduct business. That shift extends beyond technology.

Historically, operational authority, operational responsibility, and legal accountability frequently resided within the same organizational boundaries. Those exercising meaningful operational control generally assumed responsibility for maintaining that control and answered for the legal consequences when failures occurred. Existing legal doctrines, e.g., negligence, contract, agency, fiduciary obligation, statutory interpretation, and regulatory enforcement, developed relatively comfortably within that operational reality. Those doctrines remain fully capable of resolving disputes arising from modern digital operations.

What's changed however, is the operational environment within which those doctrines are applied. Modern enterprises increasingly function through relationships rather than organizational boundaries. Infrastructure may be owned or operated by or outsourced in its entirety to one or more organizations. Software developed by another, cybersecurity monitored by a managed security service provider, authentication provided through federated identity platforms, data processed across multiple cloud environments, and operational decisions increasingly informed by artificial intelligence developed and maintained elsewhere. Regulatory obligations, meanwhile, may remain with the regulated enterprise notwithstanding the delegation of operational

The author, a partner and chair of the Cybersecurity and Data Privacy practice group at Mandelbaum Barrett PC, may be contacted at steppler@mblawfirm.com.

functions, while separate obligations may also attach directly to third parties performing those functions.²

As digital operations have become progressively disaggregated, operational authority, operational responsibility, and legal accountability no longer align with the consistency, or in the manner, they once did. Organizations often retain legal accountability for operational environments over which they exercise only partial operational authority, while other participants exercise substantial operational influence without assuming (often expressly by contract) corresponding legal obligations. In one respect, responsibility has not become uncertain because legal doctrine has failed. It has become more difficult to understand – and accountably manage – because the operational relationships through which responsibility is exercised have become more numerous, more interconnected, and more persistent.

This observation is not intended to suggest that digital operations require a new body of law. Existing legal doctrines continue to provide the principles through which responsibility is allocated and disputes are resolved. Instead, it suggests that lawyers, judges, regulators, corporate boards, insurers, and organizations increasingly confront legal questions arising from operational environments that differ materially from those within which many traditional assumptions regarding organizational responsibility first developed.

The analytical challenge therefore is not whether existing legal doctrine remains adequate, but whether those doctrines are being applied with a sufficiently complete understanding of the operational environments within which responsibility now resides.

Distributed Digital Liability is offered as an analytical framework for addressing that challenge. It neither proposes a new theory of liability nor questions the continuing vitality of established legal principles. Instead, it provides a disciplined means of organizing inquiry into the operational relationships that increasingly shape legal accountability within modern digital operations. Its contribution lies not in changing the law, but in improving the analysis that precedes the law's application.

I. THE DISAGGREGATION OF DIGITAL OPERATIONS

Digital operations did not become disaggregated overnight. Modern enterprises did not consciously

redesign themselves around distributed operational responsibility. Today's operational environments emerged through thousands of individual decisions made over many years, each intended to solve an immediate business problem or improve a particular operational capability. Infrastructure migrated from on premise deployments to enterprise data centers to cloud platforms. Permanent software licenses have largely given way to software-as-a-service. Cybersecurity monitoring increasingly shifted to managed security service and SOC (Security Operations Center) providers. Open-source software has emerged as foundational to commercial applications. Identity management now expands beyond organizational boundaries through federated authentication services. Artificial intelligence increasingly supports software development, customer engagement, fraud detection, operational decision-making, and countless other business functions.

Each of these developments individually represented a rational response to changing business and technological demands. Organizations sought greater scalability, improved resilience, reduced capital expenditures, access to specialized expertise, faster software development, and more agile operational models. Few of these decisions were driven by legal considerations, nor should they have been. They reflect sound operational judgment.

Collectively, however, these decisions produced something larger than the sum of their individual benefits. Operational functions that had once been performed largely within a single enterprise became distributed across an expanding network of cloud providers, software developers, managed service organizations, software libraries, identity providers, artificial intelligence platforms, and specialized vendors. Modern digital operations increasingly depend upon these relationships, which, by design (if not overt intent) extend well beyond the traditional boundaries of any single organization.³

This distinction is important because the resulting complexity is frequently misunderstood. The defining characteristic of modern digital operations is not complexity for its own sake. Nor is it merely the increased number of technologies upon which organizations rely. Instead, it is the progressive *disaggregation* of operational functions across independent participants whose respective roles, responsibilities,

operational authority, and exposure to risk, differ significantly.

Disaggregation should not be confused with decentralization. A function may remain tightly governed while being operationally distributed among multiple participants. Nor should disaggregation be understood as a flaw in modern digital architecture. It is, in many respects, the inevitable consequence of specialization. Organizations routinely obtain greater capability, resilience, innovation, and operational efficiency by relying upon service providers possessing expertise that would be impractical or impossible to replicate internally. The legal significance of this architectural shift lies elsewhere.

As operational functions become increasingly distributed, organizations necessarily become more dependent upon relationships over which they exercise only partial operational authority. Cloud providers maintain infrastructure. Software vendors develop and update critical applications. Managed security service providers monitor enterprise environments. Identity providers authenticate users across organizational boundaries. Artificial intelligence systems increasingly inform operational decisions. Each participant performs functions that may be indispensable to the enterprise while remaining organizationally distinct from it. Operational dependence, however, should not be mistaken for operational control.

Organizations may depend extensively upon technologies and services they neither own nor directly manage. Conversely, technology providers may exercise substantial operational authority over systems supporting thousands of organizations while assuming contractual obligations and risk profiles materially different from the legal responsibilities ultimately borne by those organizations. The resulting operational environment is therefore characterized not simply by shared technology, but by shared operational influence exercised through persistent relationships extending across technological, contractual, and organizational boundaries.

Understanding this distinction is essential because it explains why questions of legal responsibility increasingly resist analysis focused upon any single participant. Modern digital operations function through an operational architecture assembled over time rather than designed as a unified whole. Responsibility therefore cannot always be understood by examining individual technologies,

vendors, or contractual relationships in isolation. It requires understanding the operational environment those relationships collectively create.

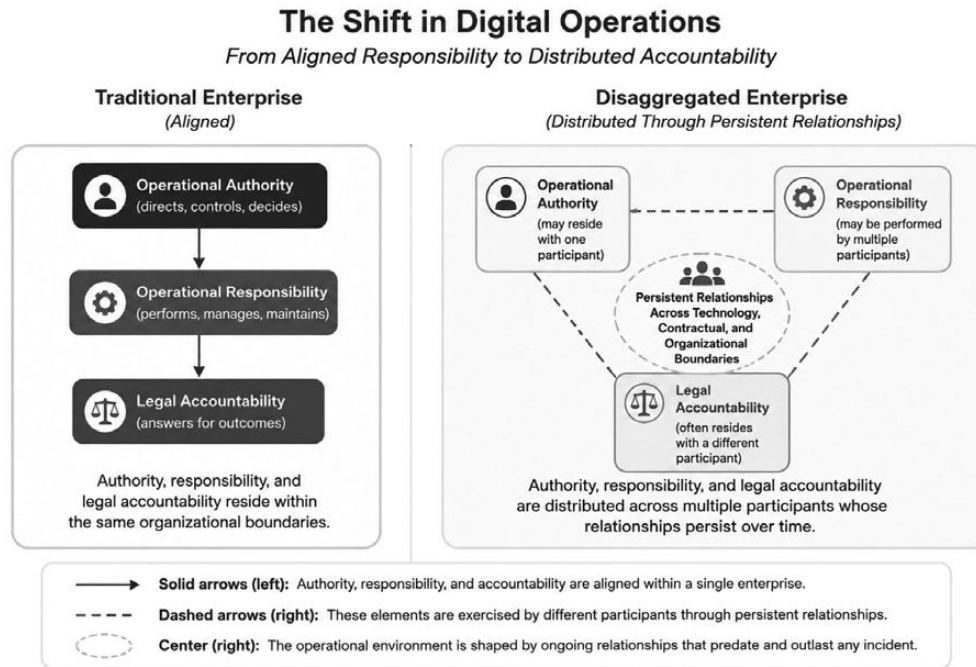
II. THE ARCHITECTURE OF RESPONSIBILITY

Responsibility is shaped by more than control. Legal responsibility has never depended upon operational simplicity. Complex commercial relationships, delegated authority, independent contractors, agency principles, contractual allocations of risk, and regulatory obligations have long required courts to evaluate conduct occurring across multiple participants. The existence of multiple actors, standing alone, presents neither a novel legal problem nor an obstacle to the application of established legal doctrine. Modern digital operations present a different challenge.

The difficulty does not arise because more organizations participate in any operational environment. It arises because the relationship among operational authority, operational responsibility, and legal accountability has become progressively less aligned as operational functions have become increasingly disaggregated. These concepts are related, but they are not synonymous. Operational authority concerns the practical ability to influence, configure, direct, or control digital operations. Operational responsibility concerns the duties assigned to maintain, monitor, secure, or administer those operations. Legal accountability addresses who ultimately answers for the legal consequences arising from those operations. Historically, these concepts frequently resided within the same enterprise. Increasingly, they do not. This distinction is more than semantic. It reflects an important characteristic of modern digital operations.

A related distinction also deserves attention. Operational authority and operational influence are not always synonymous. Operational authority generally reflects the ability to direct, configure, administer, or control a particular operational function. Operational influence, by contrast, may arise where a participant substantially affects how digital operations are performed without exercising direct operational control over the enterprise itself. Software developers influence operational behavior through application design and updates. Cloud providers influence operational resilience through infrastructure management. Identity providers

Figure 1. The Shift in Digital Operations: From Aligned Responsibility to Distributed Accountability



influence authentication decisions across organizational boundaries. Artificial intelligence systems increasingly influence operational decision-making by shaping recommendations, prioritizing responses, or automating routine functions. These participants may exercise varying degrees of operational influence without necessarily assuming corresponding operational authority or legal accountability. Recognizing this distinction further illustrates why understanding responsibility within modern digital operations requires examination of the broader operational architecture rather than exclusive focus upon any single participant.

An organization may remain legally accountable for safeguarding personal information while relying extensively upon third parties to host infrastructure, authenticate users, monitor cybersecurity events, process transactions, develop software, or support operational decision-making. Conversely, a cloud provider, managed service organization, identity provider, or software developer may exercise substantial operational authority over systems supporting thousands of enterprises while assuming contractual obligations materially different from the legal obligations borne by those enterprises. Neither

observation is remarkable in isolation. Collectively, however, they demonstrate that operational authority and legal accountability no longer align with the consistency they once did. The same observation increasingly applies to artificial intelligence.⁴

Courts and other adjudicative fora (e.g., judges, juries and arbitrators) will continue to determine negligence, contractual liability, statutory compliance, fiduciary obligation, regulatory responsibility, and damages through established legal principles.

Artificial intelligence systems may influence operational decisions affecting customers, employees, patients, financial transactions, cybersecurity operations, and regulatory compliance. Yet those systems frequently operate within governance structures in which responsibility remains distributed among developers, deployers, operators, service providers, customers, and regulated organizations. The legal questions arising from those relationships are neither identical nor necessarily

resolved by identifying the participant exercising the greatest technical influence over the system at a particular moment. What is important to recognize is that these distinctions do not alter the governing law.⁵

Courts and other adjudicative fora (e.g., judges, juries and arbitrators) will continue to determine negligence, contractual liability, statutory compliance, fiduciary obligation, regulatory responsibility, and damages through established legal principles. Those doctrines remain entirely capable of allocating responsibility among multiple participants. The analytical challenge lies elsewhere. Before those doctrines can be intelligently applied, the operational environment giving rise to the dispute must first be understood.

Understanding the operational environment (and the disaggregation of liability sources) has become increasingly important because operational authority is no longer exercised exclusively through organizational ownership or direct control. Influence over digital operations may arise through software development, infrastructure management, authentication services, artificial intelligence, contractual delegation, operational support, or countless other relationships that collectively shape how modern enterprises function. No single participant necessarily possesses complete visibility into the operational environment as a whole.

The resulting legal analysis therefore extends beyond identifying who controlled a particular technology or performed a particular operational function. It increasingly requires understanding how operational authority was exercised, how operational responsibilities were allocated, and where legal accountability ultimately resides within a broader operational architecture assembled through persistent relationships among multiple participants.

Distributed Digital Liability begins with this observation. Responsibility within modern digital operations is increasingly shaped not by isolated acts or individual technologies, but by the interaction of operational authority, operational responsibility, and legal accountability across an operational environment whose relevant relationships extend well beyond the traditional boundaries of any single enterprise. The framework's objective is to foster understanding of, rather than redefine those relationships before legal conclusions are drawn.

Distributed Digital Liability does not presume that greater operational participation produces greater legal liability, nor does it suggest that responsibility should be apportioned according to technical influence. Not every relationship within a digital environment carries equal legal significance, and distributed operations do not necessarily produce distributed ultimate liability. Existing law remains responsible for those determinations. The framework's narrower purpose is to ensure that the operational relationships potentially relevant to those determinations are identified and understood before legal responsibility is assessed.

III. PERSISTENT RELATIONSHIPS

Digital incidents reveal relationships more often than they create them. The immediate aftermath of a cybersecurity incident naturally directs attention toward the event itself. Investigators seek to identify the compromised credential, the exploited vulnerability, the software defect, the cloud service interruption, the malicious actor, or the operational failure that appears to have initiated the incident. Those inquiries are indispensable. They explain how the incident occurred. They do not necessarily explain why legal responsibility ultimately attaches where it does. The relationships that shape legal accountability frequently predate the incident itself.

These relationships arise gradually through technology acquisitions, outsourcing decisions, software integrations, cloud migrations, identity management, vendor selection, contractual allocations of responsibility, governance decisions, regulatory obligations, and countless other operational choices made over many years. Each decision appears reasonable when considered independently. Collectively, however, they produce an operational architecture within which authority is exercised, responsibilities are allocated, and legal accountability ultimately resides. The incident marks the point at which those relationships become visible – not the point at which they begin. Relationships that had quietly shaped the operational environment (and emerged without much notice or fanfare) suddenly become central to determining legal accountability.

This observation explains why significant digital incidents often appear to create legal complexity when, in reality, they expose operational relationships that had long existed. The incident compresses

years of technological, contractual, and governance decisions into a single moment of legal scrutiny. Questions that previously appeared operational become legal. Relationships that had functioned quietly during ordinary business operations become the focus of litigation, regulatory inquiry, insurance coverage analysis, contractual interpretation, and board oversight. The distinction is subtle but important. Digital incidents are episodic. The operational relationships that shape legal accountability are continuous. The legal significance of these relationships lies not in their creation by a particular event, but in their continuing existence before, during, and after that event.

The legal significance of this distinction extends well beyond incident response. An organization's dependence upon a cloud provider, software developer, managed security service provider, identity platform, artificial intelligence system, or other operational participant does not begin when a cyber incident occurs. Those relationships already influence how authority is exercised, how operational responsibilities are performed, and how legal obligations are fulfilled. The incident merely changes the questions that lawyers, regulators, insurers, and organizations begin asking about those relationships.

Recent litigation arising from the Change Healthcare cyber incident illustrates this distinction. Whatever the ultimate disposition of the claims, the legal questions extend well beyond the initiating cyber event. They implicate technology providers, healthcare entities, contractual relationships, operational responsibilities, regulatory obligations, and decisions made long before the incident itself occurred. The litigation is significant not because it announces a new legal doctrine, but because it demonstrates how understanding responsibility increasingly requires understanding the operational architecture within which that responsibility arose.⁶

Persistent relationships therefore should not be understood as hidden relationships. They are generally observable, documented, and often well understood within their individual operational contexts. What is less frequently appreciated is their cumulative legal significance. Individually, each relationship may appear routine. Collectively, they define the operational environment within which legal accountability is ultimately evaluated.

This distinction explains why modern digital disputes increasingly resist simplistic allocations of responsibility. Operational authority may be exercised by one participant, operational responsibility shared among several others, and legal accountability ultimately determined by statutory obligations, contractual commitments, common law principles, or regulatory requirements applicable to different entities altogether. None of these relationships arises because of the incident. The incident simply exposes the architecture through which they have been operating all along.

These relationships also do not operate as parallel lines. They interact. A cloud provider's configuration may affect what a security provider can observe; an identity service may determine how an enterprise control is enforced; a contractual allocation may determine which participant must act upon information generated by another. The significance of one relationship may therefore depend upon the existence, performance, or failure of another. That interaction is part of what makes disaggregated operational environments difficult to analyze and why the relevant architecture must be understood as a whole rather than as a collection of isolated vendor relationships.

Distributed Digital Liability begins with recognition of this reality. The framework assumes that legal responsibility cannot always be understood solely by examining the initiating event. It instead encourages examination of the persistent operational relationships that shaped the environment before the event occurred and that continue to influence the legal analysis after it has ended. With this perspective, the incident becomes neither the beginning nor the end of the inquiry. It becomes the point at which the operational architecture, long assembled through ordinary business decisions, is finally examined through a legal lens.

IV. ORGANIZING THE INQUIRY

Attorneys are trained to recognize that good legal analysis begins before legal conclusions are drawn. That observation may appear self-evident, yet it assumes increasing importance within modern digital operations. As operational environments become more disaggregated, legal analysis that begins by assigning responsibility to a particular participant risks overlooking the broader operational architecture from which that

responsibility arises. Distributed Digital Liability therefore proposes neither a different legal outcome nor a different legal standard. It proposes a more disciplined point of departure. This distinction, that the framework begins with the operational environment rather than the incident, is important.

Distributed Digital Liability therefore proposes neither a different legal outcome nor a different legal standard. It proposes a more disciplined point of departure.

Traditional legal analysis naturally seeks to identify the conduct giving rise to liability. In many digital disputes, however, understanding that conduct first requires understanding the operational relationships within which it occurred. Authority may have been exercised by one participant, operational responsibilities performed by another, contractual obligations allocated among several others, and legal accountability ultimately determined under statutory, regulatory, or common-law principles applicable to different entities altogether. None of those relationships can be evaluated intelligently in isolation. Accordingly, Distributed Digital Liability encourages lawyers to organize the inquiry before organizing the argument.

The framework asks a series of related questions, not because those questions are legally novel, but because modern digital operations increasingly require them. Where was operational authority actually exercised? How were operational responsibilities allocated? Which operational relationships remained significant notwithstanding organizational boundaries? Which legal obligations could be delegated operationally, and which remained legally nondelegable? How did those relationships collectively shape the operational environment within which the disputed conduct occurred?

The order in which these questions are asked and addressed matters. Legal doctrine ultimately supplies the rules by which responsibility is assigned. Before those rules can be applied effectively, however, the factual and operational environment from which the dispute arises must first be understood. The framework therefore postpones legal conclusions long enough to ensure that the operational

architecture has been accurately identified. Only then does it proceed to the application of established legal principles.

This approach does not diminish the importance of traditional legal analysis. Quite the opposite. It strengthens that analysis by ensuring that familiar doctrines are applied to a more complete understanding of the underlying operational environment. Negligence, contract, fiduciary obligation, agency, statutory interpretation, and regulatory enforcement continue to perform precisely the functions they always have. Distributed Digital Liability simply recognizes that the operational facts to which those doctrines are applied increasingly arise within distributed environments assembled through persistent relationships rather than confined within the boundaries of a single enterprise.

Distributed Digital Liability accordingly is less a methodology for reaching legal conclusions than a discipline for organizing legal inquiry. Its contribution lies not in altering the law, but in encouraging a more deliberate examination of the operational architecture from which legal responsibility ultimately emerges. The framework therefore resists the temptation to reduce digital disputes to a search for a single responsible actor. Modern digital operations rarely function through a single operational center. They function through a network of participants whose respective authority, responsibilities, contractual commitments, technological capabilities, and legal obligations frequently intersect – and interact. The objective is not to diffuse responsibility among those participants. It is to understand the operational environment sufficiently well that existing legal doctrine can allocate responsibility with greater precision.

That distinction is perhaps the framework's most important contribution. Distributed Digital Liability does not ask lawyers to think differently about the law. It asks them to think more completely about the operational environment to which the law is being applied.

V. THE FRAMEWORK IN APPLICATION

Consider a hypothetical publicly traded healthcare technology company that provides an electronic medical record and electronic health record platform to hospitals, physician practices, and other healthcare organizations. The company hosts

portions of its platform in a third-party cloud environment, relies upon a separate identity provider for authentication, uses a managed security service provider to monitor portions of its environment, incorporates third-party software components, and offers an artificial intelligence-enabled module supporting clinical documentation and coding. Its customers depend upon the platform for daily operations, while contracts, business associate agreements, service-level commitments, insurance requirements, and regulatory obligations allocate different responsibilities among the participants.

Assume that a compromised identity credential permits unauthorized access to an administrative function. The intrusion is not immediately detected. A configuration within the cloud environment affects available logging, the managed security provider receives incomplete telemetry, and a third-party software component complicates containment. The company later determines that protected health information and other personal information may have been accessed. Service disruption affects several hospital customers, contractual notice provisions are triggered, and the company must evaluate regulatory notification obligations, customer communications, insurance requirements, and, because it is publicly traded, whether the incident presents material disclosure considerations.

A conventional analysis might begin with the compromised credential or ask which participant caused the failure. Distributed Digital Liability begins one step earlier. It asks how the operational environment was assembled and how responsibility functioned within it before the incident occurred. The identity provider may have exercised operational influence over authentication without controlling the healthcare company's enterprise. The cloud provider may have exercised operational authority over portions of the infrastructure while the healthcare company retained legal obligations arising from its own role. The managed security provider may have assumed responsibility for specified monitoring functions without assuming responsibility for every control affecting detection. Hospital customers may possess their own regulatory and contractual obligations even though they did not operate the affected platform.

The framework then asks how those relationships interacted. Did the identity architecture affect the security controls available to the company? Did

cloud configuration determine what telemetry could reach the managed security provider? Did contractual commitments define who was responsible for investigating, notifying, preserving evidence, or communicating with customers? Did the company retain authority to change a control for which another participant had operational responsibility? Which obligations could be delegated operationally, and which remained with the legally accountable entity notwithstanding that delegation?

Only after the operational architecture is understood does ordinary legal analysis begin assigning consequences. Contract law may determine whether service commitments were breached or risk was allocated among participants. Statutory and regulatory requirements may determine notification, safeguarding, or reporting duties. Common-law principles may govern claims arising from alleged failures of care. Securities law may require the public company to evaluate materiality and disclosure. None of those doctrines is displaced by the framework. Nor does the hypothetical assume that liability ultimately will be distributed among all participants. The point is narrower: a legally sound conclusion depends upon understanding the different forms of authority, responsibility, influence, and accountability that existed before the event and continued through it.

The hypothetical also demonstrates why the framework has value before an incident. The same inquiry can be conducted while systems are functioning normally. Mapping who exercises authority, who performs operational responsibilities, which participants materially influence outcomes, how those relationships interact, and where legal accountability remains can expose gaps that are difficult to recognize when each contract, technology, or vendor relationship is considered separately. Distributed Digital Liability therefore provides not only a way to analyze responsibility after failure, but a way to make the architecture of responsibility more visible before failure occurs.

VI. GOVERNANCE IMPLICATIONS

Operational architecture is no longer solely a technological concern. It has become a governance concern. As organizations have become increasingly dependent upon distributed digital operations, decisions concerning technology architecture have assumed legal significance extending well beyond

the information technology function. Cloud adoption, vendor selection, software procurement, identity management, artificial intelligence deployment, cybersecurity operations, and contractual allocation of operational responsibilities increasingly influence not only how organizations function, but also how legal responsibility may ultimately be evaluated when disputes arise. This observation carries important implications for corporate governance.

Boards of directors are routinely charged with overseeing enterprise risk while relying upon operational environments assembled through numerous independent technology providers, software platforms, cloud services, and specialized vendors. General counsel negotiate contractual provisions allocating operational responsibilities among participants whose respective legal obligations frequently remain distinct. Chief information security officers implement security controls across environments they neither own nor exclusively control. Enterprise risk managers evaluate operational dependencies extending across multiple tiers of technology providers. Regulators increasingly examine governance processes that depend upon operational relationships extending well beyond the regulated entity itself. Each of these activities involves a common analytical challenge. Understanding legal responsibility increasingly requires understanding the operational architecture through which responsibility is exercised. This observation becomes critically significant before an incident occurs.⁷

Governance is often understood as a process of assigning responsibilities, adopting policies, negotiating contracts, implementing controls, and managing operational risk. Distributed Digital Liability suggests an additional perspective. Effective governance also requires understanding the persistent operational relationships through which those responsibilities will ultimately be performed. Organizations that understand those relationships before a dispute arises are better positioned to evaluate contractual risk, allocate operational responsibilities, document governance decisions, oversee third-party relationships, and respond more effectively when operational failures occur.⁸

The framework therefore possesses value independent of litigation. Its principal contribution is not simply improving the analysis of disputes after they arise. It is encouraging organizations to understand the operational architecture within which

future disputes are likely to occur. In that respect, Distributed Digital Liability functions as much as a governance framework as a litigation framework. The same inquiry that assists courts, regulators, and litigants following an incident may assist boards, executives, and counsel in understanding operational dependencies long before any incident occurs.

Recent litigation arising from the Change Healthcare cyber incident illustrates this broader point. Whatever the ultimate judicial resolution, it exposes and underscores the legal questions that extend well beyond and before the initiating cyber event. They implicate healthcare entities, technology providers, contractual relationships, cybersecurity responsibilities, regulatory obligations, operational dependencies, and governance decisions established well before the incident itself. The litigation demonstrates that understanding legal accountability increasingly requires understanding the operational architecture within which accountability was exercised before the incident occurred.

The same observation applies across industries. Financial institutions increasingly depend upon cloud providers, payment processors, identity services, and artificial intelligence supporting operational decisions. Manufacturers rely upon interconnected supply chains and operational technologies extending beyond organizational boundaries. Healthcare organizations depend upon electronic health record platforms, revenue cycle providers, managed service organizations, and cloud infrastructure. Educational institutions, retailers, insurers, critical infrastructure operators, and government agencies confront similar patterns of operational dependence. The technologies differ. The analytical challenge remains remarkably consistent.

Distributed Digital Liability does not suggest that every operational relationship carries equal legal significance. Nor does it imply that responsibility should be distributed equally among participants. Existing legal doctrine will continue to determine where legal accountability ultimately resides. The framework instead recognizes that those determinations increasingly require a more complete understanding of the operational environment before legal conclusions are reached.

The framework therefore offers a practical benefit extending beyond any individual dispute. It encourages organizations to examine operational

architecture before it is tested by litigation, regulatory inquiry, or operational failure. Relationships that appear routine during ordinary business operations often become legally indispensable when those operations are interrupted. Understanding those relationships before they are examined under the pressure of an incident is itself an important component of sound governance. The enduring value of Distributed Digital Liability therefore lies not merely in explaining digital responsibility after it has been challenged. Its greater contribution may be encouraging organizations to understand responsibility while digital operations continue to function as intended.

VII. CONCLUSION

Existing legal doctrines have not become obsolete. Instead, they are increasingly applied to factual environments assembled through operational relationships that were comparatively uncommon when many of those doctrines matured. The challenge therefore lies less in adapting the law than in understanding the operational context to which existing law is applied.

Modern digital operations are not merely dynamic by design. Each department, division or subsidiary will have its own vector and direction. In light of this, organizations will continue to reconfigure their operations as they adopt new technologies, new service models, and new operational relationships. Cloud platforms will mature. Artificial intelligence will assume new operational functions. Software supply chains will continue to expand. Specialized technology providers will perform increasingly important operational roles. The technologies themselves will change, just as they always have. The central analytical challenge, however, is unlikely to change with them.

As digital operations become increasingly disaggregated, legal responsibility will continue to arise within operational environments assembled through relationships extending through a web of technological, contractual, and organizational boundaries. Those relationships will persist whether or not they are continuously recognized. They will influence how operational authority is exercised, how operational responsibilities are performed, and where legal accountability ultimately resides. When disputes arise, those relationships will become the

subject of legal scrutiny. The incident will not have created them. It will have revealed their significance.

This observation does not diminish the continuing vitality of existing legal doctrine. Courts will continue to resolve disputes through established principles of negligence, contract, agency, fiduciary obligation, statutory interpretation, and regulatory enforcement. Legislatures and regulators will continue to refine statutory obligations in response to changing technologies and evolving public expectations. The law will continue to perform the function it has always performed. The operational environment within which that law is applied, however, has become materially different.

As digital operations become increasingly disaggregated, legal responsibility will continue to arise within operational environments assembled through relationships extending through a web of technological, contractual, and organizational boundaries.

Distributed Digital Liability is offered in recognition of that reality. It does not propose a new doctrine of law, nor does it seek to redefine the principles through which responsibility is ultimately assigned. Instead, it provides an analytical framework for understanding the operational architecture from which questions of legal responsibility increasingly arise. More importantly, it encourages a discipline of inquiry that begins with understanding persistent operational relationships before legal conclusions are drawn. That discipline may prove to be the framework's most enduring contribution.

The value of Distributed Digital Liability lies less in the terminology it introduces than in the perspective it encourages. It asks lawyers, judges, regulators, corporate directors, insurers, executives, and cybersecurity professionals to examine digital disputes with a more complete understanding of the operational environments from which those disputes emerge. It recognizes that legal accountability increasingly reflects the interaction of operational authority, operational responsibility, and persistent relationships assembled over time through ordinary business decisions rather than extraordinary technological events.

Distributed Digital Liability is essentially neither an endpoint nor a substitute for traditional legal analysis. It is an invitation to organize that analysis more deliberately. By understanding the operational architecture before assigning legal responsibility, practitioners may apply familiar legal doctrines with greater precision, greater confidence, and a fuller appreciation of the operational realities that increasingly define modern digital enterprise. If the framework encourages that discipline of inquiry, it will have served its intended purpose.

Notes

1. National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29 (Feb. 26, 2024), <https://doi.org/10.6028/NIST.CSWP.29>; Jon Boyens et al., Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, NIST SP 800-161 Rev. 1, Update 1 (May 2022, updated Nov. 1, 2024), <https://doi.org/10.6028/NIST.SP.800-161r1-upd1>.
2. See U.S. Department of Health and Human Services, Covered Entities and Business Associates (updated Aug. 21, 2024), <https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html>; 45 C.F.R. §§ 160.103, 164.502(e), 164.504(e). The HIPAA framework illustrates different and overlapping duties notwithstanding delegation. how operational functions may be performed by business associates while legal duties remain allocated by statute and regulation to covered entities and, for specified provisions, directly to business associates.
3. Jon Boyens et al., Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, NIST SP 800-161 Rev. 1, Update 1 (May 2022, updated Nov. 1, 2024), <https://doi.org/10.6028/NIST.SP.800-161r1-upd1>. NIST specifically identifies reduced visibility into how acquired technology is developed, integrated, and deployed as a source of cybersecurity supply-chain risk.
4. See 45 C.F.R. pts. 160, 164; U.S. Department of Health and Human Services, Direct Liability of Business Associates (July 16, 2021), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html>. HIPAA provides a useful example of differing but overlapping legal obligations among covered entities, business associates, and subcontractors.
5. Elham Tabassi, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1 (Jan. 26, 2023), <https://doi.org/10.6028/NIST.AI.100-1>. The AI RMF is directed to organizations designing, developing, deploying, or using AI systems and organizes risk management across governance, mapping, measurement, and management functions.
6. In re Change Healthcare, Inc. Customer Data Security Breach Litigation, MDL No. 24-3108 (DWF/DJF) (D. Minn.); U.S. District Court for the District of Minnesota, Change Healthcare, Inc. Data Breach; U.S. Department of Health and Human Services, Change Healthcare Cybersecurity Incident Frequently Asked Questions (updated Mar. 14, 2025); Chris Jaikaran, Congressional Research Service, The Change Healthcare Cyberattack and Response Considerations for Policymakers, IN12330 (Apr. 24, 2024).
7. Securities and Exchange Commission, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release Nos. 33-11216, 34-97989 (July 26, 2023), codified in relevant part at 17 C.F.R. § 229.106. The rule requires disclosure regarding processes for assessing and managing material cybersecurity risks, management's role, and board oversight.
8. See Federal Trade Commission, Safeguards Rule, 16 C.F.R. § 314.4(f); Securities and Exchange Commission, Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, Release No. 34-100155 (May 16, 2024), including 17 C.F.R. § 248.30(a)(5). The amended Regulation S-P requires covered institutions to establish written policies and procedures reasonably designed to oversee service providers, including through due diligence and monitoring, while retaining specified obligations notwithstanding use of a service provider.

Copyright © 2026 CCH Incorporated. All Rights Reserved.
Reprinted from *Intellectual Property & Technology Law Journal*, November-December 2026,
Volume 38, Number 10, pages 12–22, with permission from Wolters Kluwer, New York, NY,
1-800-638-8437, www.WoltersKluwerLR.com



Wolters Kluwer