SOUTHERN LAW JOURNAL

OFFICIAL PUBLICATION OF THE SOUTHERN ACADEMY OF LEGAL STUDIES IN BUSINESS
WWW.SALSB.ORG

VOLUME XXXIII **FALL 2025** **NUMBER 1**

SOUTHERN LAW JOURNAL

The *Southern Law Journal* is an official publication of the Southern Academy of Legal Studies in Business
ISSN: 1056-2184
ISBN: 978-1-63498-892-6
Listed in *Ulrich's International Periodical Directory* and *Cabell's Directory*
***Available at* www.southernlawjournal.com and through EBSCO, an electronic university database**

From the Editor's Desk . . .

The ***SLJ* Style Sheet** may be found at our website: www.southernlawjounal.com. If you plan to submit, please follow the *SLJ* Style Sheet closely. Contributors should visit our website for recently revised ***SLJ* Submission Policies.** Although it is expected that most *SLJ* articles will be presented at the SALSB Annual Conference, conference presentation is not a prerequisite for publication.

Hard copies of back issues of the SLJ can be found in over two hundred regional libraries. Current issues can be obtained by contacting the editor at dxb029@shsu. In addition, the full text of all *SLJ* articles may be accessed through EBSCO's "Academic Research Complete" database, accessible through over 90% of the world's Electronic University holdings.

Thank you in advance for helping the *SLJ* team continue to advance the quality, exposure, and prominence of the *SLJ* for many decades to come.

Questions and submissions should be directed to dxb029@shsu.edu

Kind regards,
Diana Brown,
Editor-in-Chief
Southern Law Journal

REPOSITORY LIBRARIES FOR THE SOUTHERN LAW JOURNAL (BACK ISSUES)

Abilene Christian University ..... Brown Library
Amberton University ..... Library Resources Center
Angelo State University ..... Porter Henderson Library
Arkansas State University of Jonesboro ..... Dean B. Ellis Library
Arkansas Tech University ..... Pendergraft Library and Technology Center
Arlington Baptist College ..... Earl K. Oldham Library
Austin College ..... George T. and Gladys H. Abell Library Center
Baylor Law School ..... Baylor Law Library
Baylor University ..... Baylor Collections of Political Materials
Baylor University ..... University Libraries
Cameron University ..... Cameron University Library
Concordia University Austin ..... Founders Library
Dallas Baptist University ..... Vance Memorial Library
East Central University ..... Linscheid Library
East Texas Baptist University ..... Jarrett Library
Grambling State University ..... A.C. Lewis Memorial Library
Harding University ..... Brackett Library
Hardin-Simmons University ..... Hardin-Simmons University Library
Henderson State University, Arkadelphia ..... Huie Library
Hendrix College ..... Olin C. Bailey Library
Howard Payne University ..... Walker Memorial Library
Lamar University Beaumont ..... Mary and John Gray Library
Langston University ..... G. Lamar Harrison Library
Louisiana College ..... Richard W. Norton Memorial Library
Louisiana State University in Shreveport ..... Noel Memorial Library
Louisiana State University Law School ..... Prescott Memorial Library
Louisiana Tech University ..... Paul M. Herbert Law Center
Loyola University New Orleans Law Library ..... The Law Library
Loyola University New Orleans ..... J. Edgar and Louise S. Monroe Library
Lyon College ..... Mabee-Simpson Library
McMurry University ..... Jay-Rollins Library
McNeese State University Library ..... Frazar Memorial Library
Midwestern State University ..... Moffett Library
Nicholls State University ..... Ellender Memorial Library
North Central Texas ..... North Central Texas College Library
Northeastern Oklahoma State University ..... John Vaughan Library
Northwestern State University ..... Watson Memorial Library
Northwood University ..... Hach Library
Ohio Northern University College of Law ..... Taggart Law Library
Oklahoma City University ..... Gold Star Library
Oklahoma Panhandle State University ..... Marvin E. McKee Library
Oklahoma State University–Stillwater ..... Edmond Low Library
Ouachita Baptist University, Arkadelphia ..... Riley-Hickingbotham Library
Rice University ..... Fondren Library
Rogers State University ..... Stratton Taylor Library
Sam Houston State University ..... Newton Gresham Library
Schreiner University ..... William Logan Library
South Texas College of Law ..... The Fred Parks Law Library
Southeastern Louisiana University ..... Linus A. Sims Memorial Library
Southeastern Oklahoma State University ..... Henry G. Bennett Memorial Library
Southern Arkansas University, Magnolia ..... Magale Library
Southern Methodist University ..... Bridwell Library
Southern Methodist University ..... Underwood Law Library
Southern University Law Center ..... Southern University Law Center Library
Southwestern Christian College ..... Doris Johnson Library
Southwestern Oklahoma State University ..... Al Harris Library
Southwestern University ..... A. Frank Smith, Jr., Library Center
St. Mary's University–San Antonio ..... Law Library
Stephen F. Austin State University ..... Ralph W. Steen Library

Supreme Court of Oklahoma ..... Supreme Court of Oklahoma Law Library
Tarleton State University ..... Dick Smith Library
Texas A & M University at Commerce ..... James G. Gee Library
Texas A & M University ..... Texas A&M Libraries
Texas A&M International University ..... Sue and Radcliffe Killam Library
Texas A&M University–Corpus Christi ..... Mary and Jeff Bell Library
Texas Christian University ..... Mary Courts Burnett Library
Texas Southern University ..... Thurgood Marshall School of Law Library
Texas State University–San Marcos ..... Texas Tech University Law Library
Texas Tech University at Lubbock ..... Law Library
Texas Wesleyan University School of Law ..... Elizabeth Huth Coates Library
Trinity University–San Antonio ..... Law Library
Tulane Law School ..... Tulane Law School Library
Tulane University ..... Howard-Tilton Memorial Library
University of Arkansas (main campus), Fayetteville ..... Young Law Library
University of Arkansas at Little Rock, Little Rock ..... Ottenheimer Library
University of Central Arkansas ..... Torreyson Library
University of Central Oklahoma ..... Chambers Library
University of Dallas ..... Blakley Library
University of Houston at Clear Lake in Houston ..... Neumann Library
University of Houston at Downtown in Houston ..... W.I. Dykes Library
University of Houston at Houston ..... O'Quinn Law Library
University of Houston at Victoria ..... University of Houston Library
University of Louisiana at Lafayette ..... Edith Garland Dupre Library
University of Louisiana at Monroe ..... University of Louisiana at Monroe Library
University of New Orleans ..... Earl K. Long Library
University of North Texas ..... University of North Texas Libraries
University of OK College of Law ..... Donald E. Pray Law Library
University of Oklahoma ..... Bizzell Memorial Library
University of Texas at Arlington ..... Central Library
University of Texas at Austin ..... Tarlton Law Library
University of Texas at Richardson ..... McDermott Library
University of Texas at Tyler ..... Robert R. Muntz Library
University of Texas– San Antonio ..... University of Texas San Antonio Library
University of Texas– San Antonio Downtown ..... University of Texas San Antonio Downtown Library
University of Texas–El Paso .....The Library
University of Texas–Pan American–Edinburg ..... University Library
University of the Ozarks ..... L.S. and Hazel C. Robson Library
University of Tulsa College of Law ..... Mabee Legal Information Center
University of Tulsa–Tulsa, Oklahoma ..... McFarlin Library
Wayland Baptist University ..... Wayland Library
West Texas A&M University ..... Cornette Library
Xavier University ..... Library Resource Center

SALSB EXECUTIVE COMMITTEE
(2025)

NEGOTIATION COURSES AND THE EXPANDED VIEW OF BUSINESS LAW PEDAGOGY

EVAN PETERSON*

Legal departments within organizations are increasingly moving from a traditional, reactive approach toward a proactive, holistic approach in line with growing recognition of legal strategy as a critical component to risk management and organizational value creation. Proactive law encapsulates an innovative relationship between the organization and its legal department centered on using law and legal strategy as empowering mechanisms cultivate value and manage risk.[1] Efforts to integrate legal strategy into broader organizational practices through the promotion of proactive law require an examination of key concepts in change management, including organizational politics, political skill, influence tactics, and emotional intelligence. In-house counsel with political astuteness stand in a strong position to navigate the resulting organizational dynamics and promote proactive law perspectives to yield positive outcomes for the legal department and the organization.[2] The need for political astuteness signifies a new paradigm in an expanded view of business law pedagogy: preparation for real-world practice must extend beyond the traditional delivery of black letter law to more fully integrate cross-disciplinary skills, knowledge, and perspectives. Institutions that include negotiations courses within undergraduate business law curricular requirements will position their students to develop a range of critical interdisciplinary skills connected to in-house legal practice: assertiveness, empathy, flexibility, social intelligence, and ethicality.[3]

This paper proceeds in several parts. Part I introduces proactive law within the context of an expanded view of legal strategy. Part II provides an overview of foundational concepts in organizational management affecting the promotion of proactive law perspectives, including organizational change, organizational politics/power relations, influence tactics, political skill, and emotional intelligence. Part III encompasses a discussion of political astuteness, a concept that illustrates the connection between the foundational concepts in organizational management and the in-house practice of law. Part IV examines the role of negotiation courses within the expanded view of business law pedagogy, alongside the associated accreditation benefits. Part V describes the methodology and assignments for a negotiation strategies & tactics course taught from the expanded view of business law pedagogy at the University of Detroit Mercy. Part VI details student learning results and instructor observations from the course. Part VII concludes with a summary of the implications addressed by this paper.

---

* Evan A. Peterson, JD, PhD, Arnold Jarboe Chair of Business Administration, Director of Center for Practice & Research in Management & Ethics (PRIME Center), University of Detroit Mercy, Detroit, MI. petersea@udmercy.edu

[1] Gerlinde Berger-Walliser & Paul Shrivastava, *Beyond Compliance: Sustainable Development, Business, and Proactive Law*, 46 GEO. J. INT'L. L. 418, 434 (2015).

[2] For the present article, political astuteness refers to the ability of promotors of proactive law, through high levels of emotional intelligence, to understand that the perspectives, behaviors and motives of others reflect differences in skills, values, attitudes, and goals.

[3] Andrea Kupfer Schneider, *Teaching A New Negotiation Skills Paradigm*, 39 WASH. U. J.L. & POL'Y. 13, 28-35 (2012).

I. PROACTIVE LAW AND THE EXPANDED VIEW OF LEGAL STRATEGY

A. Background on Proactive Law

The foundational purposes of the legal department involve avoiding value destruction and promoting value creation. These foundational purposes are achieved through advocating and fostering legal awareness throughout the organization, developing legal solutions aligned with organizational goals, and using appropriate legal measures in response to business risks.[4] An increasing number of legal departments are embracing best practices from other business functions.[5] For example, in-house counsel are playing greater roles in sustaining organizational strategic value and bearing new responsibilities in sync with the growing respect for law as a source of organizational value creation.[6] In-house counsel now serve as crisis managers in greater numbers,[7] demanding fresh levels of insight toward organizational strategic objectives and the solutions best aligned with achieving those objectives.[8]

An increasing number of organizations are beginning to recognize the value of forward-thinking, coordinated, interdisciplinary responses to legal challenges. There is tremendous value in promoting legal astuteness within the organization.[9] Proactive law encapsulates an innovative relationship between the organization and its legal department centered on using law and legal strategy as empowering mechanisms cultivate value and manage risk.[10] The aim of proactive law is to support the company's competitive strategy by integrating future-oriented legal strategy principles into the organization's guiding policies and action plans.[11] Proactive law includes the following core elements:[12]

- supporting compliance with applicable legal rules and regulations;
- minimizing the risks, problems, and losses associated with non-compliance;
- eliminating the chief causes of compliance failures;
- lawyers serving as strategic advisors;
- assisting in the attainment of mutual goals and objectives;

---

[4] Christine Pauleau et al., *Key Performance Indicators (KPIs): Run Legal with Business Metrics: Will the Legal of the Future Measure Everything It Does?* in *Liquid Legal* 111-128 (Kai Jacob, Dierk Schindler, & Roger Strathausen 1 ed. 2017).

[5] Liam Brown et al., *Running the Legal Department with Business Discipline: Applying Business Best Practices to the Corporate Legal Function*, in *Liquid Legal* 397-421 (Kai Jacob, Dierk Schindler, & Roger Strathausen 1 ed. 2017).

[6] David Orozco, *Strategic Legal Bullying*, 13 N.Y.U. J. L. & BUS. 137, 138 (2016).

[7] Constance E. Bagley & Mark Roellig, *The Transformation of General Counsel: Setting the Strategic Legal Agenda*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2201246

[8] Bjarne P. Tellmann & Susan R. Sneider, *The Relationship Between the Legal Department and the Corporation*, § 16:2. The Evolving Role of the General Counsel, SUCCESSFUL PARTNERING BETWEEN INSIDE AND OUTSIDE COUNSEL ((ROBERT HAIG ED., 2021).

[9] Pauleau et al., *supra* note 1.

[10] Gerlinde Berger-Walliser & Paul Shrivastava, *Beyond Compliance: Sustainable Development, Business, and Proactive Law*, 46 GEO. J. INT'L. L. 418, 434 (2015).

[11] George J. Siedel & Helena Haapio, *Using Proactive Law for Competitive Advantage*, AM. BUS. L. J. 641, 641 (2010).

[12] Berger-Walliser & Shrivastava, *supra* note 7.

- maximizing the positive benefits and outcomes of upcoming business opportunities;
- driving impending business success factors, and
- promoting the involvement of lawyers in cross-professional collaborative teams.

Scholars have incorporated proactive law principles into a variety of frameworks designed to increase the acknowledgement of legal strategy as an integral element of overall organizational strategy. For example, the Manager's Legal Plan (MLP) encompasses four steps geared toward supporting proactive managerial perceptions toward law and legal strategy: (1) understanding the legal dimensions of business and learning how to work alongside legal professionals; (2) recognizing ways to deal with legal problems by handling their costs and learning from the challenges they create; (3) developing business solutions to prevent legal problems from occurring again in the future; and (4) reframing legal problems as business opportunities to develop new options for value creation.[13] The Legal Astuteness framework places a heavy focus on proactive attitudes toward legal regulation by emphasizing: (1) value-laden attitudes toward the value of law to business success; (2) proactive attitudes toward legal regulation; (3) informed judgment in managing legal issues that affect the business, and (d) the use of suitable legal tools in conjunction with context-specific legal knowledge.[14] Concept-Sensitive Managerial Analysis enables managers to grasp the effect of legal regulations on business decisions through: (1) applying business concepts to legal regulations to detect conditions that will promote business opportunities; (2) identifying environmental conditions that will not afford flexibility to exploit business opportunities; and (3) applying a legal-analytical methodology in the decision-making process to ensure compliance with legal requirements.[15] Although these frameworks approach proactive law from different perspectives, they each contribute to reducing perceived silos between 'legal' and 'business' considerations.

B. Resistance to Proactive Law

Efforts to encourage proactive law within an organization (or department) require acknowledgement and consideration of the perspectives held by those asked to implement its principles. Notwithstanding the prospective advantages of the proactive law approach, its proponents have faced resistance from those within and outside the legal department. A core tenet of proactive law focuses on collaboration between managers, lawyers, and other subject matter experts.[16] As discussed in section II, differences in skills, values, attitudes, goals, and behaviors can lead to conflict.[17] Numerous sources of potential conflict exist regarding managerial perspectives toward proactive law. For example, managers may view lawyers as anti-team players, a necessary evil, and incapable of creative problem solving.[18] Some managers may view law as

[13] GEORGE J. SIEDEL & HELENA HAAPIO, PROACTIVE LAW FOR MANAGERS: A HIDDEN SOURCE OF COMPETITIVE ADVANTAGE (2016).
[14] Constance E. Bagley, *Winning Legally: The Value of Legal Astuteness*, 33 ACAD. MGMT. REV. 378, 379 (2008).
[15] *Id.*
[16] Berger-Walliser & Shrivastava, *supra* note 7.
[17] *Id.*
[18] Chuck Barry & Kristin Kunz, *In-House Counsel should Implement Servant Leadership to Help Clients make Values-Based Decisions*, 37 HAMLINE L. REV. 501, 519 (2014); Robert L. Nelson & Laura B. Nielsen, *Cops, Counsel, and Entrepreneurs: Constructing the Role of Inside Counsel in Large Corporations*, 34 L. & SOC. REV. 457, 468 (2000).

hindrance organizational growth,[19] while others may view legal concerns as the exclusive responsibility of in-house counsel.[20] The perspectives, goals, and positions of in-house counsel also raise potential sources of conflict. The results of one study highlighted several key obstacles that may present sources of conflict, such as the belief that it is not the job of in-house counsel to support the views, perspectives, and interests of others.[21] The results of the study also revealed concerns by in-house counsel that supporting the views, perspectives, and interests of others could lead in-house counsel to suppress their own independent judgment.[22] These perspectives and the ensuing conflicts may hinder efforts to promote collaboration and impede the advancement of proactive law principles across the organization.

Although resistance to proactive law from some managers may come as little surprise, resistance to proactive law from in-house counsel is farther outside the realm of expectation. It is important to remember, however, that proactive law envisions a new (and different) relationship between the legal department and the organization as compared to a more traditional reactive relationship.[23] This relationship may signify a major departure from the current practices of many legal departments. Prior research involving differences in perspectives among in-house counsel may offer some clarification as to the variation in receptivity to proactive law perspectives. Nelson and Nielsen identified three, non-mutually exclusive types of in-house counsel:[24]

- *cop* – concerned primarily w/policing business client's conduct; disinclined to offer non-legal advice even where opportunities occur.
- *counsel* – plays key role in placing lawyers within business activities; maintains broader relationship w/business actors that provides opportunities to render non-legal advice (based on business, ethical, and situational concerns).
- *entrepreneur* – emphasizes business values; views law as source of profits; perceives role as going far beyond providing legal advice.

The variations in perspectives and approaches emanating from the different types of in-house counsel will inevitably obstruct efforts to build momentum and consensus in the promotion of proactive law perspectives within the legal department (and by consequence across the organization). Other research provides further context for the potential challenges proponents of proactive law may face from within the legal department. Results from a study on building consensus among in-house general counsel to address managerial legal strategy perspectives revealed concerns regarding the feasibility and desirability of legal departments engaging in different practices connected to the proactive law perspective, including business process engagement by in-house counsel, departmental revenue generation, and the use of performance

[19] Siedel & Haapio, *supra* note 10.
[20] Robert C. Bird, *The Many Futures of Legal Strategy*, 47 AM. BUS. L.J. 575, 581 (2010).
[21] Evan A. Peterson, *Building Consensus Among General Counsel to Address Managerial Legal Strategy Perspectives* (Nov. 2017) (unpublished Ph.D. dissertation, Walden University) (on file with ProQuest Dissertations Publishing).
[22] *Id.*
[23] Susie Lees et al., *Stop Putting out Fires and Start Working Proactively with your Client*, 31 ACC DOCKET 73, 77 (2013).
[24] Nelson & Nielsen, *supra* note 15.

metrics.25 It is therefore essential to also address unreceptivity from within the legal department itself when contemplating changes that include proactive law principles. For proactive law perspectives to take hold within a legal department (and the larger organizations), changes from past and present practices may be necessary. The next section will introduce foundational concepts in organizational management related to the change process.

II. FOUNDATIONAL CONCEPTS IN ORGANIZATIONAL MANAGEMENT

A. Organizational Change

Any attempt to promote proactive law perspectives within the legal department may represent a considerable change from past and present departmental practices. Resistance created from organizational conflict is a significant factor in the failure of any change initiative.[26] Organizational conflict arises in the presence of several driving forces: (a) unshared attitudes, values, skills, behaviors, or goals that direct another person's behavior; (b) obligations to perform an action that is unrelated to a person's needs; or (c) different behavioral preference regarding a collective action.[27] Strategies and techniques are often necessary to modify values, beliefs, attitudes, or structures within an organization if a change initiative is to succeed.[28] This is known as organizational change. A central challenge in implementing organizational change rests on finding suitable mechanisms for considering the diverse viewpoints that accompany the change process. As noted by Bolman and Deal, structural,[29] human resource,[30] symbolic,[31] and political[32] dimensions (frames) accompany any organizational change. All four frames are vital to the success of any change initiative.[33] The next section will focus on organizational politics, power relations, and influence tactics through the lens of the political frame.

B. Politics, Power Relations, and Influence Tactics

Organizational politics denotes an unescapable element of organizational dynamics. Bolman and Deal liken organizations to arenas, characterized by a continuous interplay of players and agendas: organizations set the rules of the game, the stakes, and the parameters for players.[34] Organizational politics encompass actions taken within an organization connected to the acquisition, development, and deployment of power and other resources to achieve desired

---

[25] Evan A. Peterson, *Building Consensus Among General Counsel to Address Managerial Legal Strategy Perspectives* (Nov. 2017) (unpublished Ph.D. dissertation, Walden University) (on file with ProQuest Dissertations Publishing).
[26] Afzalur M. Rahim, *Toward a Theory of Managing Organizational Conflict*, 13(3) INT'L J. CONFLICT MGMT. 206, 206 (2002).
[27] *Id.*
[28] WARREN G. BENNIS, ORGANIZATIONAL DEVELOPMENT: ITS NATURE, ORIGINS, AND PROSPECTS (1969); TOM E. BURNS & G.M. STALKER, THE MANAGEMENT OF INNOVATION (1961).
[29] LEE G. BOLMAN & TERRENCE DEAL, REFRAMING ORGANIZATIONS: ARTISTRY, CHOICE, AND LEADERSHIP (2017) at 48.
[30] *Id.* at 118.
[31] *Id.* at 241.
[32] *Id.* at 184.
[33] *Id.* at 381.
[34] *Id.* at 218-220.

personal outcomes.[35] Every organizational process has a political dimension.[36] Opposing interests, resource scarcity, and power relations drive organizational politics.[37] Such driving forces are a permanent fixture withing organizational dynamics. As such, every department and member of the organization must learn to identify, understand, and respond to the necessary dynamics presented by organizational politics.[38] As divergent interests, scarcity, and power relations denote the driving forces of organizational politics,[39] power and organizational politics will always be intertwined.

A core nexus exists between power and organizational politics. This nexus rests on techniques used by opposing groups and individuals to articulate their preferences and achieve their goals.[40] Some scholars suggest that organizational politics involve the use of self-serving influence behaviors that are often detrimental to the organization.[41] Other scholars, however, suggest that organizational politics denote a common, acceptable, socially functional phenomenon that can assist in organizational goal attainment.[42] The ability to achieve organizational goals is characterized by a shared relationship between subordinates and superiors, each person maintaining the capacity to influence the other in support of proper functionality.[43] Power represents a person's (agent's) inferred potential to cause another person (the target) to perform according to the agent's desires.[44] French and Raven (1959) identified numerous sources of power, including (a) legitimate power – based on prerogatives, obligations, and responsibilities connected to formal positions in organizations;[45] (b) reward power – based on agent's capacity to reward target;[46] (c) expert power – based on expertise, ability, and/or knowledge of agent;[47] (d) referent power – based on target's identification with agent;[48] and (e) coercive power – based on agent's ability to punish target or prevent target from obtaining desired rewards.[49]

Influence tactics, efforts to alter other's perspectives and actions, embody the essence of power. An understanding of influence processes within the organization supports an understanding of: (a) why organizations adopt some innovations but not others; (b) likelihood of implementing strategies and policies successfully; and (c) overall decision-making in organizations.[50] The respective works by Kipnis and Schmidt (1985) and Falbe and

---

[35] J. Pfeffer, *Management as Symbolic Action: The Creation and Maintenance of Organizational Paradigms*. In L.L. Cummings and B.M. Staw (eds), *Research in Organizational Behavior* (Vol. 3, pp. 1–52). Greenwich, CT: JAI Press (1981).
[36] *Id.*
[37] Bolman & Deal, *supra* note 27 at 183.
[38] *Id.*
[39] Bolman & Deal, *supra* note 27 at 183.
[40] Bolman & Deal, *supra* note 27 at 190.
[41] Amos Drory & Tsilia Romm, *The Definition of Organizational Politics – A Review*, 43 HUMAN RELATIONS 1133–54 (1990).
[42] ERAN VIGODA-GADOT, DEVELOPMENTS IN ORGANIZATIONAL POLITICS (2003).
[43] Chad A Higgins et al., *Influence Tactics and Work Outcomes: A Meta-analysis*, 24 J. ORG. BEHAV., 89, 103 (2003).
[44] BERNARD M. BASS, BASS AND STOGDILL'S HANDBOOK OF LEADERSHIP: THEORY, RESEARCH, AND MANAGERIAL APPLICATIONS (1990).
[45] John R. P. French & Bertram Raven, *The Bases of Social Power*. In D. Cartwright (Ed.), *Studies in Social Power.* Ann Arbor: Institute for Social Research, University of Michigan (1959).
[46] *Id.*
[47] *Id.*
[48] *Id.*
[49] *Id.*
[50] Cecilia M. Falbe & Gary Yukl, *Consequences for Managers of Using Single Influence Tactics and Combinations of Tactics*, 35 ACAD. MGMT. J., 638, 644 (1992).

Yukl (1992) represent two of the seminal works in this field. Kipnis and Schmidt (1985) identified three categories of influence behavior:[51]

- *soft strategy* encompasses gratifying and empathizing with target person to achieve compliance in a polite, friendly, or humble manner.
- *hard strategy* involves efforts to gain compliance using direct, assertive requests, manipulative threats, and aggression.
- *rational strategy* entails offering alternatives to target person that maximize value of outcome(s) important to the target, on condition(s) that target comply with influence request(s).

Falbe and Yukl (1992) identified nine influence tactics involving an assortment of influence behaviors:

- *inspirational appeal* - arousing enthusiasm by boosting target person's confidence that they can perform requested action(s) or by appealing to target person's values, beliefs, or interests.
- *coalition tactics* - enlisting aid or endorsement of others to influence target person.
- *rational persuasion* - using logical arguments and factual evidence to convince target person of action's value.
- *consultation* – seeking participation in planning action(s) for which target person's support is needed, as well as modifying proposal(s) to accommodate target person's input and worries.
- *ingratiation* - seeking to elevate the target person's mood or view toward person making request(s).
- *exchange tactics* - offering exchange of favors, reciprocation at later date, or shared benefits if target person completes action(s).
- *personal appeal* – guiding target person to perform action(s) as special favor by appealing to target person's feelings of loyalty and friendship.
- *pressure tactics* - using ultimatums, coercion, or constant reminders to influence target person.
- *legitimating tactics* – legitimizing request(s) by asserting authorization or by asserting consistency with organizational policies.

The 'successful' deployment of influence tactics within the organization necessitates the consideration of several important factors. Those seeking to influence others must weigh the suitability of a particular influence tactic (or combination of tactics) given the needs of the situation. The use of influence tactics can evoke negative emotional reactions among the recipients of those tactics.[52] Use of pressure tactics, for example, can produce anger, resentment, and fear among the target(s) of such pressure.[53] The indiscriminate use of influence tactics can lead to

[51] Stuart Schmidt & David Kipnis, *The Language of Persuasion*, 4 PSYCH. TODAY, 40, 40 (1985).
[52] *See, e.g.,* Anthony P. Ammeter et al., *Toward a Political Theory of Leadership*, 13 LEADERSHIP QUARTERLY, 751 (2002).
[53] Cecilia M. Falbe & Gary Yukl, *Consequences for Managers of Using Single Influence Tactics and Combinations of Tactics*, 35 ACAD. MGMT. J., 638, 644 (1992).

potentially disastrous and far-reaching unintended consequences throughout a department (or organization). Those seeking to deploy influence tactics successfully must acquire and grow their political skill.[54]

C. Political Skill and Emotional Intelligence

Political skill represents a critical component to navigating the waters of organizational politics. Political skill denotes a person's capacity to understand others at work and to use this understanding to influence others in ways that enhance the person's personal and/or organizational objectives.[55] As noted by Ferris et al., there are four key dimensions of political skill:[56]

- *social astuteness* – individuals attuned to social interactions allowing for accurate interpretation of their behavior and others' behavior.
- *interpersonal influence* – individuals capable of eliciting desired responses from others by adapting their behavior in response to others' behavior.
- *networking ability* – individuals adept at developing friendships and building beneficial alliances.
- *apparent sincerity* – individuals perceived (by the target of influence) as possessing high levels of sincerity, authenticity, integrity, and genuineness.

The definition and dimensions of political skill suggest that understanding others is critical to effective influence.[57] Individuals with political skill understand the perspectives, behaviors and motives of others, thus developing a sense of when/how to apply influence tactics for maximum effect.[58]

Understanding the perspectives, behaviors and motives of others demands a significant level of emotional intelligence. Individuals with a high level of emotional intelligence are positioned to predict the emotional effects/responses of any influence attempts from their potential influence targets.[59] As noted by Lynn, the formulation of emotional intelligence in the context of group dynamics encompasses the following elements: (a) self-awareness/self-control – understanding oneself and using that information to manage emotions; (b) empathy – understanding others' perspectives; (c) social expertness – building genuine relationships and expressing caring, concern, and conflict in healthy ways; (d) personal influence – positively leading/inspiring others; and (e) mastery of purpose/vision – living out one's intentions and values.[60] Study results suggest a positive relationship between emotional intelligence and political skill.[61] The connections between emotional intelligence and political skill have important implications for efforts to promote proactive law perspectives throughout an organization.

---

[54] Higgins, et al., *supra* note 40 at 90.
[55] Gerald R. Ferris et al., *Development and Validation of the Political Skill Inventory*, 31 J. MGMT., 126, 127-128 (2005).
[56] *Id.*
[57] *Id.*
[58] Gerald R. Ferris et al., *Political Skill in Organizations*, 33 J. MGMT. 290, 314-315 (2007).
[59] Galit Meisler, *Exploring Emotional Intelligence, Political Skill, and Job Satisfaction*, 36 EMPLOYEE RELATIONS 280, 288 (2014).
[60] ADELE B. LYNN, THE EQ DIFFERENCE: A POWERFUL PLAN FOR PUTTING EMOTIONAL INTELLIGENCE TO WORK (2004).
[61] Meisler, *supra* note 56.

III. DEVELOPING POLITICAL ASTUTENESS

Organizational politics is an inescapable aspect of legal department operations. The expectations placed on in-house counsel and the legal department to fuel the power relations and scarcity that drive organizational politics.[62] Promoting proactive law perspectives in step with the evolving legal department expectations necessitates a recognition of the strategies and tactics used by opposing groups and individuals to articulate their preferences and achieve their goals. Although the elimination of organizational politics is impossible, it is possible to understand (and thus attempt to manage) the ensuing political dynamics within the legal department and across the organization.[63] A major challenge in developing this understanding, however, rests on the fact that promotors of proactive law may lack the preparation, capacity and comfort needed to use influence tactics in ways perceived as yielding positive outcomes.[64] Growing scholarship on emotional intelligence in the practice of law provides a possible means to develop the capacity and comfort necessary for achieving positive outcomes through the deployment of influence tactics. Emotional intelligence is a core competency essential to success in modern in-house legal practice.[65] Acknowledging the role of emotions in the legal process assists attorneys in making better decisions, embracing change, and recognizing social cues.[66] Elements of emotional maturity are present within fundamental lawyering skills, including problem solving, the resolution of ethical dilemmas, and negotiation.[67]

Promotors of proactive law with high levels of emotional intelligence are uniquely positioned to make proactive law a reality. As noted in section I, efforts to encourage proactive law require acknowledgement and consideration of the perspectives held by those asked to implement its principles. Although a core tenet of proactive law focuses on collaboration between managers, lawyers, and other subject matter experts,[68] differences in skills, values, attitudes, goals, and behaviors between these individuals can lead to conflict.[69] These ensuing conflicts may hinder efforts to promote collaboration and impede the advancement of proactive law principles within the legal department and across the organization. In-house counsel with political astuteness stand in a strong position to overcome resistance impeding the implementation of proactive law principles. Through this understanding, in-house counsel can manage political dynamics by using influence tactics to yield positive outcomes for the legal department and the organization: the promotion of proactive law perspectives. The next section will discuss how courses in negotiation provide an ideal learning environment for developing political astuteness.

---

[62] Bolman & Deal, *supra* note 26 at 178.
[63] Bolman & Deal, *supra* note 26 at 183-184.
[64] Weinstein et al., *Teaching Teamwork to Law Students*, 63 J. L. EDUC. 36 (2013) (Teamwork concepts are infrequently taught in legal education).
[65] Terri Mottershead & Sandee Magliozzi, *Can Competencies Drive Change in the Legal Profession?* 11 UNIV. ST. THOMAS L. J. 51, 61 (2013).
[66] *See* Dana L. Joseph et al., *Why Does Self-Reported Emotional Intelligence Predict Job Performance? A Meta-Analytic Investigation of Mixed EI*, 100 J. APPLIED PSYCHOL. 309 (2015); Kihwan Kim et al., *Emotional Intelligence and Negotiation Outcomes: Mediating Effects of Rapport, Negotiation Strategy, and Judgment Accuracy*, 24 GROUP DECISION & NEGOTIATION 487 (2015).
[67] Randall Kiser, *The Emotionally Attentive Lawyer: Balancing the Rule of Law with the Realities of Human Behavior*, 15 NEV. L. J. 442, 445 (2014).
[68] Berger-Walliser & Shrivastava, *supra* note 7.
[69] *Id.*

IV. NEGOTIATION COURSES IN HIGHER EDUCATION

A. Negotiation and the Expanded View of Business Law Pedagogy

The days of the legal department operating in an insulated silo separate from the rest of the organization are long gone. Responses to legal crises now require a seamless combination of business acumen, legal knowledge, and negotiation skills, requiring an increasingly interdisciplinary approach to the practice of law. In-house counsel routinely find themselves working alongside individuals with diverse perspectives, behaviors, values, and goals.[70] Although a solid foundation in business law concepts is a critical first step, the holistic preparation for real-world business practice must extend beyond the traditional delivery of black letter law.[71] Such an expanded view of the scope of the business law discipline supports the inclusion of business law related course offerings within concentrations in marketing, accounting, finance, information systems, and human resource management.[72] Just as the silos between legal and business issues are eroding, so too are the silos between academic disciplines. Courses in negotiation provide business law students with the opportunity to consider a range of skills connected to the field and practice of law, including the importance of body language and building one's professional reputation. Negotiations courses also provide students with an opportunity to examine biases in their decision-making, an important component to the business law discipline. Students' awareness of biases will better position them to address potential biases in their actions and decision-making.[73] Social influences, emotional motivations, and unconscious reactions can undermine rational decision-making and mislead decision-makers into believing that they have made rational decisions.[74] Most importantly, however, negotiation courses provide students with the opportunity to improve conflict resolution and practical negotiation skills, supporting their development of a foundation in political astuteness. Business law faculty are uniquely suited to advance and support student's practical application of these broader cross-disciplinary skills, knowledge, and perspectives.[75] In this capacity, business law faculty assist with the curricular innovations necessary to ensure their institutions meet accreditation requirements focused on preparing students to meet the changing needs of the business world.

---

[70] Robert Waterman & Bruce E. Yannett, *Crisis Management*, SUCCESSFUL PARTNERING BETWEEN INSIDE AND OUTSIDE COUNSEL (2018 (crisis management teams routinely include managers, executives, directors, outside counsel, and outside consultants).

[71] Evan A. Peterson, *Crisis Management in Legal Environment Courses*, 24 ATLANTIC L.J. 201, 201 (2022).

[72] O'Brien et al., *supra* note 1.

[73] *See, e.g.,* George F. Loewenstein et al., *Risk as Feelings*, 127 PSYCHOLOGICAL BULLETIN. 267 (2001); Hans-Rüdiger Pfister & Gisela Böhm, *The Multiplicity of Emotions: A Framework of Emotional Functions in Decision Making*, 3 JUDGMENT AND DECISION MAKING. 5 (2008); X. T. Wang et al., *Social Cues and Verbal Framing in Risky Choice*, 14 J. BEHAVIORAL DECISION MAKING. 1 (2001); Eldad Yechiam et al., Observing Others' Behavior and Risk Taking in Decisions from Experience. 3 JUDGMENT AND DECISION MAKING. 493 (2008); Laura A. Kaster, Improving Lawyer Judgment by Reducing the Impact of "Client-Think." 67 DISP. RES. J. 56 (2012).

[74] *See, e.g.,* George F. Loewenstein et al., *Risk as Feelings*, 127 PSYCHOLOGICAL BULLETIN. 267 (2001); Hans-Rüdiger Pfister & Gisela Böhm, *The Multiplicity of Emotions: A Framework of Emotional Functions in Decision Making*, 3 JUDGMENT AND DECISION MAKING. 5 (2008); X. T. Wang et al., *Social Cues and Verbal Framing in Risky Choice*, 14 J. BEHAVIORAL DECISION MAKING. 1 (2001); Eldad Yechiam et al., Observing Others' Behavior and Risk Taking in Decisions from Experience. 3 JUDGMENT AND DECISION MAKING. 493 (2008); Laura A. Kaster, Improving Lawyer Judgment by Reducing the Impact of "Client-Think." 67 DISP. RES. J. 56 (2012).

[75] Robert C. Bird & Cheryl Kirschner, *Special Report: The Summit on the Academic Profession of Business Law*, 37 J. LEGAL STUD. EDUC. 87, 91 (2020).

B. Accreditation Benefits of an Expanded View of Business Law Pedagogy

Addressing political astuteness in negotiation courses at the undergraduate level also provides benefits from an accreditation standpoint. As noted in the AACSB Guiding Principles and Standards for Business Accreditation, business schools have a responsibility to adapt to the changing needs of the business world through providing relevant skills and knowledge to the communities they serve.[76] AACSB's mission is to foster engagement, accelerate innovation, and amplify impact in business education by establishing standards for strategic management and innovation, learner success, and thought leadership, engagement, and societal impact.[77] AACSB standards reflect, "a higher calling to the purpose of business schools to make a difference in the world through positive societal impact."[78] As further noted in the AACSB Guiding Principles and Standards for Business Accreditation, the combined effect of these standards, when met across all AACSB-accredited schools, "moves AACSB toward achieving its vision of transforming business education for positive societal impact and its belief that business is a force for good in society."

Incorporating negotiation courses into undergraduate business law programs will help institutions satisfy two important standards in learner success among other standards: standard 4 and standard 7. Under standard 4, institutions must promote experiential learning.[79] Although every negotiation course is uniquely different, common threads among such courses include: (1) presentation of key negotiation theory and concepts; (2) experience conducting negotiations (via simulations, role plays, case studies, or 'live' negotiations outside class); (3) reflection on negotiation experiences; and (4) use of conceptual materials, experiences, and reflection to from new in preparation for future negotiations.[80] These common threads, based on Kolb's Experiential Learning Model (ELM), call attention to the critical importance of experience in the learning process.[81] The combination of theory and practice empowers students to learn from their experiences by making theory relevant using experiential learning.

Standard 7 encompasses the second standard supported by the incorporation of negotiation courses into business law programs. Under standard 7, institutions must provide forward-looking, globally oriented, and innovative curricular content.[82] As noted previously, AACSB standards endeavor to represent a higher calling for business schools to make a positive social impact in the world.[83] Integrating social issues into the curriculum improves students' critical thinking, tolerance, and social integration.[84] In pursuit of this standard, some business schools are focusing

---

[76] *2020 Guiding Principles and Standards for Business Accreditation*, ASSOCIATION TO ADVANCE COLLEGIATE SCHOOLS OF BUSINESS, https://www.aacsb.edu/-/media/documents/accreditation/2020-aacsb-business-accreditation-standards-jul-1-2022.pdf?rev=b40ee40b26a14d4185c504d00bade58f&hash=9B649E9B8413DFD660C6C2AFAAD10429 (last visited Sep. 27, 2024).

[77] *Id.*

[78] *Id.*

[79] *Id.*

[80] Roy J. Lewicki, *Teaching Negotiation: The State of The Practice*, in *Handbook of Conflict Management Research* 493-508, 502 (Oluremi B. Ayoko, Neal M. Ashkanasy, & Karen A. Jehn 2014).

[81] David A. Kolb, *Management and the Learning Process*, 18 CALIF. MGMT. REV. 21, 21 (1976). (Learning occurs via a four-stage cycle. Immediate concrete experience provides a basis for reflective observation. Reflective observations are then integrated into a theory through which new inferences are realized. The realized inferences serve as guideposts in creating new experiences).

[82] *2020 Guiding Principles and Standards for Business Accreditation, supra* note 71.

[83] *Id.*

[84] Nicole Fournier-Sylvester, *Daring to Debate: Strategies for Teaching Controversial Issues in the Classroom*, http://collegequarterly.ca/2013-vol16-num03-summer/fourniersylvester.html (last visited Sep. 30, 2024).

on how organizations conduct business through the lens of sustainable development.[85] Sustainable development education must also promote the ability to work with stakeholders with conflicting interests to find a common goal.[86] Negotiation courses provide the opportunity for students to develop skills critical to working with others. As discussed more fully below, negotiation courses can help students develop skills needed to work with others through developing a range of skills connected to emotional intelligence, including empathy, flexibility, social intuition, and ethicality.[87] These interdisciplinary skills are critical to the practice of law.

The next section will introduce a course in negotiation strategies & tactics that I taught recently as part of the College's business law concentration. It is my hope that this paper will provide further support for the effectiveness of teaching negotiations through negotiation simulations and illustrate the benefits of including negotiations courses within business law curricular requirements under the expanded view of business law pedagogy.

V. NEGOTIATION STRATEGIES & TACTICS – COURSE OVERVIEW

A. Course Introduction and Methodology

The course in negotiation strategies & tactics was offered for the first time in winter 2024. The course was developed to further enhance practice-oriented course offerings inspired by Constance Bagley's recognition that "optimal business school education should be interdisciplinary, active, and experiential."[88] The course was offered as part of the College's business law concentration and framed from the expanded perspective toward business law pedagogy. With this philosophy in mind, course outcomes centered on the successful application of skills to new situations.[89] Course development focused on role-play simulations, echoing the prevailing approach to teaching negotiation courses.[90] In developing the course, I was mindful of existing critiques toward the effectiveness of negotiation courses as summarized by Lewicki (2014).[91] Lewicki outlined an approach taken by Andrea Kupfer Schneider in response to critiques toward negotiation course effectiveness.[92]

Professor Schneider's approach to teaching negotiation centers on what negotiators need to do to be effective. Schneider proposed evaluating the effectiveness of teaching negotiations by evaluating the following skills:[93]

---

[85] *An Inspirational Paradigm for Jesuit Business Education*, INTERNATIONAL ASSOCIATION OF JESUIT UNIVERSITIES, https://iaju.org/working-groups/newparadigm-jesuit-business-education (last visited Sep. 30, 2024).
[86] Ann Dale & Lenore Newman. *Sustainable Development, Education and Literacy*, INT'L. J. SUSTAINABILITY IN HIGHER EDUC. 351, 351 (2005).
[87] Schneider, *supra* note 3.
[88] Constance E. Bagley et al., *A Path to Developing more Insightful Business School Graduates: A Systems-based, Experimental Approach to Integrating Law, Strategy, and Sustainability*, 19 ACAD. MGMT. LEARNING & EDUC., 541, 552 (2020).
[89] Schneider, *supra* note 3 at 37 (Focusing on skills provides students with goals for improvement based on awareness of strengths and weaknesses).
[90] Lewicki, *supra* note 75.
[91] *Id.* (Evidence not clear that students effectively learn, retain, and transfer skills from simulation exercises to new situations).
[92] Andrea Kupfer Schneider is Professor of Law and Director of the Dispute Resolution Program at Marquette University Law School.
[93] Schneider, *supra* note 3.

- Assertiveness: person's ability to assert themselves in a negotiation depends on their alternatives, goals, research/knowledge on topic, and ability to speak persuasively.
- Empathy: person's ability to express empathy in a negotiation involves a combination of skills, including open-mindedness, excellent listening, curiosity, and a willingness to hear the other side.
- Flexibility: person's ability to get the job done in terms of their ability to make strategic choices and reach flexible outcomes.
- Social intelligence: person's social awareness and social facility, including their ability to present themselves to others.
- Ethicality: person's trustworthiness and willingness to follow the ethical rules, alongside the person's perception of ethicality (reputation).

Developed based on Schneider's experience training lawyers and non-lawyers, this method of evaluation is based on the central premise that effective negotiators need to choose skills that are appropriate given the client, context, and counterpart.[94] Such a framework allows negotiators to consider past interactions, reputation, and potential future dealings, as well ponder how their skills will intermingle with skills possessed by the opposing side(s).[95] Approaching negotiation through this lens provides students with a "sophisticated understanding of the evolving and nuanced process of negotiation."[96] I adopted this assessment criteria for the negotiation strategies & tactics course, given the similarity between Schneider's approach to teaching negotiation and my articulation for an expanded perspective toward business law pedagogy. See appendix A for more information on the evaluation criteria for each skill.

B. Course Assignments

The course delivery employed various instructional methods to appeal to diverse learning styles. The central core of the negotiation strategies & tactics course rested on three types of experiential active-learning assignments: negotiation simulations, negotiation analyses, and a real-world negotiation project.[97] Mini lectures, assigned readings, group discussions, and quizzes were used to supplement fundamental concepts covered in the experiential active-learning assignments.

1. Negotiation Simulations

Over the course of the semester, students engaged in a series of increasingly complex negotiation simulations covering a wide range of business situations. Students completed five in-person simulations and two virtual simulations in one-on-one, two-on-two, group and other formats.[98] See Appendix B for a list of simulation descriptions as provided on the iDG website. Students were assigned partners and opponents in some simulations and allowed to choose their partners and opponents in other simulations. Each simulation consisted of three phases: planning phase, simulation phase, and debriefing/reflection phase. In the planning phase, students were

[94] *Id.* at 13.
[95] *Id.* at 36.
[96] *Id.* at 37.
[97] As the present paper focuses on assessing the effectiveness of negotiation simulations, the real-world negotiation project will be covered in a future paper.
[98] Students accessed simulation materials through the iDecisionGames (iDG) platform website available at https://idecisiongames.com/ Registration for the iDG platform was required for participation in the course

given general instructions (the same for all students) along with instructions specific to their roles. Students completed negotiation planning documents where they analyzed their needs, priorities, alternatives, and cutoff points to develop a strategy and tactics for the negotiation. During the simulation phase, students completed role-play simulations using materials accessible through the iDecisionGames (iDG) platform. I recorded all in-person simulations using the audio/video recording capabilities of the College's smart classroom.[99] During the debriefing/reflection phase, I would connect the simulations to course materials via class discussion, pose questions to students, and solicit comments and observations from students regarding their performance and the performance of their classmates. Within 48 hours of completing each negotiation simulation, students submitted debrief reflections exploring their impressions, reflecting on insights gained, and establishing goals for future simulations. Debrief reflections provided students with critical notes in preparation for the course's two negotiation analysis assignments.

2. Negotiation Analysis Assignments

Students completed two negotiation analysis assignments as part of the negotiation strategies & tactics course. These assignments required students to thoroughly examine, assess, and reflect on their performance during two in-person negotiation simulations completed during the semester.[100] Each assignment consisted of three components: a self-critique; a peer critique, and a discussion of best practices and takeaways. As part of the self-critique, students were required to revisit their negotiation planning documents and debrief reflections, as well as review the video recordings of their negotiation group made during each simulation. The smart classroom cameras provided students with the opportunity to review their behaviors, interactions, and performance during these simulations from multiple angles. Students were asked to reflect on their performance in as much detail as possible. As part of the peer critique, students evaluated the simulation behaviors, interactions, and performances of the other students in their respective negotiation groups. Students were asked to consider how the behaviors, interactions, and performances of others affected their own behaviors, interactions, and performances during the simulation. For the discussion on best practices and takeaways, students related three course concepts of their choosing to the simulation. Students were asked to consider assertiveness, empathy, flexibility, social intelligence, and ethicality in each of the negotiation analysis assignments. The next section will discuss student responses and reflections observed from students' submitted negotiation analysis assignments.

VI. NEGOTIATION STRATEGIES & TACTICS – RESULTS AND OBSERVATIONS

A. Results

The negotiation analysis assignments provided an immense volume of information for evaluating students' beginning skill level and progression along the five assessed skills for assertiveness, empathy, flexibility, social intelligence, and ethicality. Although it is impossible to discuss the full range of student responses in this section, I attempt here to select quotes and examples to illustrate student learning across the assessed skill levels. When possible, examples

[99] Smart Classroom enables faculty to study group interactions first-hand through audio and video recording. Students recorded the two virtual simulations using tools in Blackboard Collaborate.

[100] To assist in pre and post assessment, students submitted the first negotiation analysis during the beginning of the semester and the second negotiation analysis paper at the end of the semester.

are provided from both the first and second paper submitted by the same student to illustrate learning progression. Students did not always revisit or address the same concepts in both papers. It is important to note here that I've made judgment some calls on where to locate certain quotes and examples within the five skills areas. Although students were instructed to reflect on their skills in the five areas, they were not asked to do so in specifically labeled sections. As different students would have different experiences relative to each of the skills areas during any given simulation, I wanted students to focus on providing a thorough, reflective self-analysis instead of worrying excessively about having "something to say" in each area.

1. Assertiveness

Students provided a range of self-reflections on their assertiveness during negotiation exercises throughout the semester. In his first paper, one student remarked, "I think I demonstrated almost flawless planning and a strong understanding of my goals." He noted further how his drive for competition often takes over and expressed his belief that a lot of people want to take the easy way rather than fight and compete. In his second paper, however, he acknowledged the importance of finding common ground in negotiations alongside a need to control his competitive spirit based on the needs of the situation. The recorded videos enabled another student to identify specific instances where she hesitated to assert her needs and concerns during negotiations, leading her to acknowledge a pattern of agreeing with group decisions at the expense of her own needs and priorities. She recognized that some behavioral changes can be difficult and, "do not happen instantly." In contrast, another student expressed pride in observing her, "guard slowly diminish as she grew more comfortable in the negotiations." The video recordings allowed her to observe her body language during the negotiations, specifically how she would "get fidgety" or "crack a nervous laugh or smile" when nervous or unsure how to respond. This allowed her to control these behaviors in future negotiations. Another student commented that her voice would grow louder as she became more persistent. She noted that as her voice grew louder, she began repeating the same conditions to her opponents. She commented further as to how this indicated she was desperate for a resolution. Yet another student expressed "I sometimes underestimate the importance of thorough research and planning before entering negotiations." She went on to say, "This lack of preparation can leave me struggling to articulate my positions effectively, missing opportunities to create value, and feeling unprepared to handle unexpected challenges." In her second paper, however, this same student indicated she approached the negotiation better prepared with a specific plan of attack. Although she observed slight nervousness and some stuttering at the start of the negotiation, the tone of her voice revealed that she grew more confident and assertive as the conversation progressed. She began offering compromises toward the end of the negotiation if they could do certain things "her way."

2. Empathy

Students' reflections on their willingness to listen, open-mindedness, and other skills connected to empathy yielded a variety of insights. In his first paper, one student indicated that his competitive drive seriously took over in the final stages of the negotiation, challenging his ability to engage in active listening and to acknowledge the concerns and perspectives of the other parties. In his second paper, however, he expressed a recognition how his evolving skills as an active listener aided negotiation discussions. He found that by taking a supportive role where he listened to his opponents and teammates led to a more enjoyable, engaging experience. Another student acknowledged a need to focus less on her own arguments and suggestions and focus more on

actively listening to her opponent's concerns and asking clarifying questions when appropriate. In her second paper, this same student acknowledged that she gained insights into the significance of, considering multiple viewpoints and finding common ground in uncertain and rapidly changing circumstances. For her, the negotiation experience, . . . "highlighted the need for agility and creative problem-solving in negotiation practices. Although another student initially believed he balanced assertiveness with empathy in adapting his strategy as needed, his views on his negotiation performance evolved after viewing the recorded negotiations. The recordings allowed him to observe how he tended to "dominate the conversation," limiting his negotiation partner's opportunity to contribute and hindering effective collaboration and problem-solving. He indicated further that although he maintained a respectful attitude toward his negotiation partner, he could have been more proactive in building a positive relationship to facilitate better communication and cooperation. Another student acknowledged how the negotiation experience reinforced the importance of adaptability and flexibility from everyone involved. He acknowledged that all parties, himself included, could have been more open to compromise and creative solutions.

3. Flexibility

Students gained a unique awareness of their strengths and weaknesses in terms of their ability to "get the job done" in a negotiation setting. One student acknowledged how the behavior of her negotiation partners affected her own behavior during the simulation. She noted how she became "more heated and loud" in response to the 'aggressive tactics' of her teammates, behaviors outside her usual style. She further observed that there is a ". . . fine line between being confident and coming off as pushy." The student indicated how she would continue to work on finding balance in her approach. Another student commented that prior to her first negotiation involving multiple parties, she found herself approaching each negotiation the same way. She noted that her first experience negotiating with multiple parties was the most difficult negotiation she had encountered all semester due to the challenges posed by diverse emotions and attempts to exert power. The experience allowed her to learn "new skills to deal with stubborn opponents." A different student remarked how he assumed that negotiating with friends would be much easier than negotiating with strangers. He acknowledged that he failed to consider how his friend and negotiating opponent would not let friendship stand in the way of the negotiation. One student felt that although his client-specific instructions for a negotiation hindered his ability to achieve the 'highest points,' he still felt the process was conducted fairly and emphasized sound reasoning and strategic decision-making. Concerns regarding role-specific instructions were also raised by another student, who felt that her performance was limited by the restrictions of her role despite intensive preparation and planning. This same student expressed frustration in perceiving that her opponents without the same role-specific instructions were less willing to work together to find a mutually agreeable solution. Another student expressed admiration toward the creativity taken by his opponent in helping find a solution that worked for all parties. The student commented how his opponent proposed an "outside the box" solution at a critical point where both sides were nearing impasse and unwilling to budge further.

4. Social Intelligence

Student acquired new understandings of how the ability to present themselves to others is critical in negotiations. One student remarked that her opponent had a "good poker face," making it hard to determine whether he was lying or trying to hide information. The student commented that her opponent was aggressive in his approach and rarely open to compromise. Although she

stated these aggressive, non-compromising behaviors angered her, she still expressed a respect for her opponent's approach. Another student commented that although he did not think about non-verbal communication during a three-party negotiation, the importance of body posture and table spacing became readily apparent upon reviewing his behaviors in the recorded video. The student observed further that his body language, spacing, and other non-verbal behaviors reflected a subconscious intent to form an alliance with one of his negotiating opponents against the other, "to create a 2v1 scenario." Another student expressed how a "conversational negotiation is much easier than a fiery one." He noted further that, "taking extra steps to listen to the backgrounds of others can create an opportunity to build a conversational tone for the negotiation." another student commented how her performance during the simulations reinforced the need for identifying common ground, generating creative solutions, and striving for mutually beneficial agreements. She expressed a desire to do her best to maintain a collaborative approach geared toward win-win outcomes whenever possible. A different student surprise when negotiating against an opponent with whom she maintained a friendship outside of class. Although her opponent indicated "This is going to be easy because I'm good with compromise," before the negotiation began, the student felt her opponent's unwillingness to compromise was completely unreasonable and unexpected. One student praised her opponent, noting the opponent was a skilled and formidable counterpart who brought an elevated level of professionalism and strategic acumen to the table. The student further commented that her opponent's collaborative and empathetic nature, "significantly contributed to the overall effectiveness of our dialogue." This same opponent, in reflecting on her own performance, noted expressed that "being open to adjusting my approach based on the situation and the other party's responses is crucial for achieving a successful outcome."

5. Ethicality

Trustworthiness, a willingness to follow the rules, and the perception of one's ethicality (reputation) are instrumental to effective negotiations. One student reflected on the importance of maintaining a high level of collaboration, trust, and focus on achieving mutually beneficial outcomes. One student expressed how a request for transparency and a free flow of information made by her opponents at the start of one negotiation helped to create a sense of honesty and trust. The request helped to express the fact that the parties shared a common goal that they wanted to achieve, "as fairly as possible." In evaluating his own performance, one student commented he could have done a better job negotiating given his opponent's lack of knowledge regarding a key fact in the negotiation. He noted further that it, "is not always about making the right choice but rather making the most profit." One student commented on her need to constantly work on her ability to manage her emotions, stay composed under pressure, and empathize with the perspectives of others. She indicated this enabled her to build rapport and trust. She recognized that a sole focus on winning could lead her to overlook opportunities for collaboration and to employ adversarial tactics (deception, manipulation, etc.) which could damage relationships and undermine trust. One student remarked that after a class session discussing outcomes for a particular negotiation, it became clear to her that she had "low-balled" her opponent. The student commented further that although she technically "won" the negotiation because of the "low-ball" offer, she did not feel good about it. She further expressed a desire to "obtain favorable outcomes based on persuasion skills rather than deception skills." In describing this same negotiation, her opponent expressed frustration after discovering the "low-ball" offer. Rather than express hostility and anger, however, the recipient of the "low-ball" offer instead commented on her own preparations. The student noted essentially that had she gone into the negotiation with precisely

identified goals and points of resistance based on thorough research and understanding of industry standards, she would not have fallen for the 'misleading' tactics. Another student commented how she was sometimes too trusting in her expectation that her opponents would also desire win-win solutions. She had to adapt to their "more competitive selfish" approach as a result. She remarked on her feelings of anger and confusion after observing her opponents' behaviors through the video recordings, noting that in future negotiations she would refuse to argue and go in circles with her competitors.

B. Observations

A course debriefing session took place during the final class session of the semester. During this class session, I shared summary feedback from my observations during the negotiation simulations and insights learned from students' submitted work throughout the semester. Given the extensive use of role-play simulations in the course, I had concerns that some students would not take their artificial roles seriously based on a perception that role-play simulations are not "real-life." During the first week of the course, I reminded students that the skills and behaviors they would practice throughout the term would translate unequivocally to real experiences in both their personal and professional lives. At the end of the semester, I was very pleased overall by students' preparation and engagement in the simulations throughout the semester. The Housemates and COVID Conversations simulation was the only simulation during the semester where students expressed (and I observed) challenges in embracing the mindsets required by their artificial roles. In this simulation, students were assigned to roles with different levels of risk tolerance toward certain behaviors and activities in connection with on-campus living arrangements during the J 1 (worst) to 10 (best) immediately following each negotiation simulation. Students were asked to reconsider their ratings after viewing the recorded negotiations in connection with the two negotiation analysis assignments. Many students consistently gave themselves ratings of 8 or higher, commonly with the proviso statement that there is "always room for improvement." Although some students reduced their ratings after viewing the recordings, a sizeable number of students indicated their ratings did not change after viewing the videos. These ratings opened the door for a discussion on choice-supportive bias and social desirability bias, among other biases.[101] This could have been the result of Choice-supportive bias – positive feelings toward decision despite awareness of inherent flaws.[102]

As the negotiation strategies & tactics course was taught as part of our business law concentration, it was also critically important to discuss the course's role/relationship to the concentration during our final session. To help connect the course to the discipline and practice of business law, we discussed how to extrapolate skills learned and developed during the simulations to the practice of business law within an organizational context. Using crisis management as an example, I asked students to consider how the perspectives, ideas, and behaviors of crisis management team members (in-house counsel, managers, executives, directors, etc.) might lead to challenges in responding to the crisis. We discussed the importance of considering prior

---

[101] Nicole Bergen & Ronald Labonté, *Everything is Perfect, and We Have No Problems: Detecting and Limiting Social Desirability Bias in Qualitative Research*, 30 QUAL. HEALTH RESEARCH, 783-792 (2020) (Social desirability bias refers to the tendency to present oneself and one's social context in a way that is perceived to be socially acceptable but not wholly reflective of reality).

[102] *See, e.g.,* Samantha Lee & Shana Lebowitz, *20 Cognitive Biases that Screw Up Your Decisions*, http://www.businessinsider.com/cognitive-biases-that-affect-decisions-2015-8 (last visited Apr. 15, 2018) (Choice-supportive bias refers to positive feelings toward decision despite awareness of inherent flaws).

interactions, reputation, future interactions, and skills of the other parties in any 'negotiation' setting. Students noted how the importance of tone, asking questions, building rapport, and expressing a willingness to listen are important in any situation. One student remarked to the effect that, "At the end of the day you can't forget that you all work for the same company. Things that might work in court might not be appropriate for discussions with coworkers." Students seemed to understand and enthusiastically acknowledge the connection between course simulations and the business law discipline/practice of law. When I asked whether students would have preferred more simulations with a specific, clearly identifiable legal focus (such as simulations involving litigation, regulatory discussions, etc.), one student commented to the effect that he liked seeing examples that related to different contexts. The consensus among the students seemed to reflect an appreciation for the transferability of the negotiation skills practiced during the semester and a deeper understanding of the interdisciplinary nature of the practice of law.

VII. CONCLUSION

The days of the legal department operating in an insulated silo separate from the rest of the organization are long gone. Responses to legal crises now require a seamless combination of business acumen, legal knowledge, and negotiation skills, requiring an increasingly interdisciplinary approach to the practice of law. With the increasing recognition of legal strategy as a critical component to risk management and organizational value creation, legal departments are positioned to further develop innovative relationships within the organization. To better achieve this increased integration, however, there is a greater need to understand the challenges and pitfalls that accompany changes to past or present organizational practices. Efforts to integrate legal strategy into broader organizational practices through the promotion of proactive law require an examination of key concepts in change management, including organizational politics, political skill, influence tactics, and emotional intelligence. To put it simply, preparation for real-world practice must extend beyond the traditional delivery of black letter law to more fully integrate cross-disciplinary skills, knowledge, and perspectives. Institutions that include negotiations courses within undergraduate business law curricular requirements will position their students to develop a range of critical interdisciplinary skills connected to in-house legal practice: assertiveness, empathy, flexibility, social intelligence, and ethicality. Incorporating negotiation courses into undergraduate business law programs will help institutions promote experiential learning along with providing forward-looking, globally oriented, and innovative curricular content.

APPENDIX A[103]

Skill Description	Minimal Skill Level	Average Skill Level	Best Practice Skill Level
Assertiveness	some level of competence and knowledge	full research and preparation	confidence based on competence and knowledge
Empathy (willingness to hear other side)	distinguish between rare win-lose negotiations and those offering joint gain	ability to find integrative potential	translate parties' interests into realistic integrative proposals
Empathy (asking questions)	ask questions to get information to help move process along	ask questions to uncover counterpart's interests and needs	learning conversation to better understand counterpart's client and situation to propose solutions responding to those needs
Empathy (listening)	let other side explain their case without interrupting	ask questions when done to clarify and demonstrate one's listening.	active listening to confirm you accurately understand their perspective and respect their position (even if you don't agree)
Flexibility (strategic choices)	choosing style based on context or counterpart	shifting strategy or tactics in course of negotiation to respond to counterpart	careful thinking about reputation of counterpart; selecting skills on that basis as well as own skill set and client's situation; and adapting skills as needed based on counterpart and newly acquired information in course of negotiation
Flexibility (creative outcomes)	knowing priorities to allow for trade-offs at negotiating table	preparing one or two tradeoffs	examine variety of creative processes before and during negotiation that could provide additional solutions
Social intelligence (setting tone of negotiation)	have basic greeting	set better tone via food or ambiance	conscious attempt to enter negotiation in good mood and actively work ensure other side similarly situated
Social intelligence (setting rapport)	have level of cordiality	schmooze w/other side (ask questions and break ice)	conduct advance research to find areas of commonality and be genuinely friendly & curious
Ethicality (willingness to follow ethical rules)	follow professional rules of responsibility and not actively deceive other side	view possible deceptive behavior through lens of likely ramifications including your reputation	act trustworthy and treat other side fairly
Ethicality (trustworthiness)	create calculus-based trust between oneself and counterpart	develop knowledge-based trust where repeated interactions create predictable responses	strive for identification-based trust where parties create mutual understanding of other's needs and can act on that behalf
Ethicality (defending against lack of ethicality)	assume others might lie to you and contemplate what you can do about that	asking defensive questions to double check assertions and writing compliance measures into the contract	building a sufficiently strong relationship so that it is more difficult for others to lie to you

[103] Adapted from Schneider, *supra* note 3.

APPENDIX B[104]

Salary Negotiation – Designed to teach participants the value of negotiating package deals versus negotiating issue by issue, the effects of ego, quality of information on the negotiating strategy, and the importance of maintaining a good relationship. Participants must prioritize issues and uncover each others interests in order to reach a balanced agreement. Connects course to their careers as on why people don't negotiate salary. Also answer questions like: what should I do if they ask what salary I expect? What to do if they ask what I made in my previous job. What should I do if the salary is lower than expected?

Three Party Coalition – The Three Party Coalition is a short three-party scoreable negotiation among representatives of three organizations over the integrative and distributive aspects of a possible 2- or 3-party coalition. Three independent organizations, "A," "B" and "C," have sent representatives to a three-way negotiation. The representatives have learned that there are benefits to working together. If all three groups reach an agreement, benefits totaling 121 points will be split three ways (to be determined by the participants). If only two of the organizations reach an agreement, the total benefits to be split will be less than 121 and the third party will be left with nothing.

Housemates and COVID Conversations – This multi-party, multi-issue negotiation is set in the context of the COVID-19 global pandemic. The exercise involves three university student housemates negotiating an agreement for their house rules as the students return to campus during the pandemic. It includes a mix of distributive, integrative, and compatible issues. Housemates are each provided a unique points system to calculate their individual gains but are not provided all options for all issues; thus, there is "missing" information across roles that participants must discover and address on their own. The housemates' perspectives are informed by their different backgrounds and experiences in their home regions as well as differences in risk perceptions and tolerances. There is no strong power hierarchy among the three housemates; each plays a unique role compared to the others. The exercise involves dynamics of coalition building, tradeoffs, influence and persuasion, objective and subjective value, and managing the unique social pressures when negotiating in a personal rather than professional setting. Opportunities to form coalitions on one or more issues exist between all possible pairings.

Texoil – This is a qualitative negotiation over the sale of some property. The exercise has no overlapping bargaining zone unless the parties uncover some of each other's interests. It is a very good exercise for teaching about interests, what information should and should not be shared, and creativity in negotiations.

Tipal Dam – This is a transactional negotiation between a construction company and a foreign government. Tipal Dam is useful for teaching negotiation ethics in a cross-cultural context.

[104] Visitors to the iDG website Library (https://idecisiongames.com/v4/library) may view simulation descriptions without signing up for an account.

Harborco – This is a multi party, multi-issue, quantified negotiation. Harborco wishes to develop a deep-water port on the eastern seaboard. Attending the meeting are representatives of the governor, unions, environment, and other parts of the federal government. Most solutions are Pareto optimal. It is useful for discussing group leadership and the role of the individual parties in attempting to maintain the status quo

Public Health of Climate Change – A seven-party role-play simulation involving a diverse set of stakeholders who must consider the short-term and long-term public health impacts of climate change while assessing the pros and cons of specific (and conflicting) risk management strategies. Mapleton, a city of 100,000, has just completed a Climate Vulnerability Assessment. The assessment shows that extreme heat and possible flooding associated with climate change pose substantial threats to the city. City officials asked an Advisory Group to suggest ways of preparing for possible emergencies and preventing injury and loss of life. The Advisory Group will have to wrestle with different risk management strategies and come to agreement if they want to have an impact. This is a seven-party role-play simulation involving city officials, university planners, business representatives, and environmentalists trying to figure out how their city should respond to the possible public health impacts of climate change. The exercise introduces a public health orientation that is often lacking from local efforts to figure out how to adapt to climate risks. Participants must consider the short-term and long-term public health impacts of climate change while assessing the pros can cons of specific (and conflicting) risk management strategies.

ESSENTIAL QUESTIONS FOR SPORTS LAW: A TEACHING STRATEGY

J.M. LONG*

I. INTRODUCTION

In 2023, Professors DeMartini and Kao surveyed sports law instructors to discover determine most common sports law course topics.[1] DeMartini and Kao found that Title IX of the Education Amendments Act of 1972 ("Title IX")[2] and negligence were the two most covered substantive legal topics.[3] The survey also found that 36 different substantive sports law topics were included by at least 50 % of the survey respondents.[4] Of the 36 topics, nine (25 %) can broadly be classified under torts,[5] eight (22.22 %) broadly under employment law,[6] and seven (19.44 %) under discrimination.[7] Some survey topics cross into two broader categories. For example, "employment contracts" may be categorized under both employment and contracts.

DeMartini & Kao's study is useful because of its focus upon the specific, hard skill, knowledge critical for a course in sports law. But, as a 2024 survey by Rosenberg & Pack found, instructors recognize that sport management students must simultaneously develop "soft skills."[8] Soft skills are universal and transferrable and include the ability to critically think.[9] For both student growth and overall career success, sport management faculty consider soft skill development as equally important as hard skill development.[10] Further, the faculty perspective on soft skills matches that of potential student employers.[11]

---

* JD, MBA, Assistant Professor of Business Law, Walker College of Business, Appalachian State University

[1] Anne L. DeMartini & Pin Hung Kao, *Sport Law in U.S. Undergraduate Sport Management Programs: What Should We Be Teaching?*, 33 J. HOSP., LEISURE, SPORT, & TOURISM EDUC. 100455 (2023).

[2] 20 U.S.C. §§ 1681 et. seq.

[3] DeMartini & Kao *supra* note 1, at 4-5 (finding that 100 % of the survey respondents included Title IX coverage and 96. 3 % included coverage of "negligence - defenses").

[4] *Id.*

[5] *Id.* at 4. (The topics under torts included: negligence – defenses, negligence – waivers & releases, negligence – elements, negligence – parties' liability, negligence – premises liability, intentional torts – assault & battery, intentional torts – defamation, negligence – products, and hazing).

[6] *Id.* at 4. (including: employment contracts, the American with Disabilities Act (ADA), Title VII of the Civil Rights Act (Title VII), Equal Pay Act, age discrimination in employment, labor under the National Labor Relations Act, labor under the Fair Labor Standards Act, and insurance/worker's compensation).

[7] *Id.* at 4. (Including: Title IX of the Education Amendments of 1972, ADA, Title VII, Equal Pay Act, Equal Protection, age discrimination in employment, and Title II of the Civil Rights Act (Title II)).

[8] Jonathan Rosenberg & Simon N. Pack, *Faculty Perceptions of Soft and Hard Skills in Sport Management Curricula*, 1 THE COSMA J. 1 (2024).

[9] *Id.,* at 2; Jessica Braunstein-Minkove, et al., *Transferable Skills in Sport Management Education*, 17 SPORT MGMT. EDUC. J. 135, 136 (2023).

[10] Rosenberg & Pack, *supra* note 8, at 7.

[11] Braunstein-Minkove *supra* note 9, at 136 ("Employers now expect graduates to have highly valued transferable skills, such as problem-solving, teamwork, communication, leadership and management, and critical thinking, along with their technical abilities.").

Instructors see the value in developing both hard and soft skills but often find both difficult to deliver.[12] Various teaching strategies now offer ways to develop both hard and soft skills.[13] This article adds to the pedagogical scholarship focused upon both hard and soft skill development in the sports management curriculum. The article introduces an adaptation of the essential questions teaching strategy (EQTS) for sports law, with a particular focus upon complex problem-solving and critical thinking. The purpose and design of EQTS is to provide instructors with the ability to cover important content while also challenging students to think through complex problems, including those from the real world. While other academic disciplines, including business, history, English, physics, chemistry, mathematics, and music, have adopted EQTS,[14] sports law pedagogy does not, to my knowledge, utilize EQTS.

This article will introduce EQTS to develop the sports law curriculum. The article is divided into four parts. Part II will provide an overview of EQTS. This will include a focus upon its purpose and attention to the components of EQTS. Part III will then use the top two topics from DeMartini & Kao's list of most important topics to cover in sports law, Title IX and negligence, and provide teaching guides using EQTS. Part IV will conclude the article.

II. THE ESSENTIAL QUESTIONS TEACHING STRATEGY

EQTS is a curriculum development and delivery strategy. In both development and delivery, the strategy centralizes the "big ideas" of a discipline or topic.[15] It also encourages a focus upon creating curriculum relevant to students and increasing student engagement.[16] Wilhem summarizes that:

> "Essential questions create a problem orientation that leads to exciting learning conversations, to creative problem solving, and to the consolidation of major concepts, connections, vocabulary, strategies, and ideas that can then be used to

[12] Emily Danes-Staples, *Constructing a Sport Management Classroom*, 7 SPORT MGMT. EDUC. J. 25, 26 (2013); Logan Schuetz, et al., *Student Speed Dating as a Catalyst for Creative Idea Generation in Sport Management Programs, 2* THE COSMA J. 1, 2-3 (2025)(recognizing that teachers balancing curriculum demands have limited time to support students in creative thinking); *See* also, DeMartini, *supra* note 2, at 9 (stating that "sports law instructors do have to make compromises in the content they include.").

[13] Danes-Staples, *supra* note 12, 26 (arguing for a constructivist approach to course development); Schuetz *supra* note 12, at 1 (incorporating speed dating into classroom and online lessons); Jennifer S. Anderson, et al., *Insights from Snowboard Pedagogy for the Legal Studies Instructor*, 16 DePaul J. Sports L. 225 (2020);

[14] Michael E. Cafferky, *"Why Do We Have to Learn This Stuff?": Revising or Developing a Course Using Essential Questions*, 1 J. EXCELLENCE IN BUS. EDUC. 1 (2014)(business); Robb Virgin, *Connecting Learning: How Revisiting Big Idea Questions Can Help History Classrooms*, 105 THE SOCIAL STUDIES 201 (2014)(history); Heather Lattimer, *Challenging History: Essential Questions in the Social Studies Classroom*, 72 SOCIAL EDUC. 326, 326 (2008)(history); Doug Lillydahl, *Questioning Questioning: Essential Questions in English Classrooms*, ENGLISH J. 36 (2015)(English); Nancy Emerson Kress, *6 Essential Questions for Problem Solving*, 111 MATHEMATICS TEACHER 191 (2017)(mathematics); Gregory DiLisi, et al., *Thorium and Molten Salt Reactors: Essential Questions for Classroom Discussions*, 56 PHYSICS TEACHER 253 (2018)(Physics); Ming Chi, et al., *Reframing Chemical Thinking Through the Lens of Disciplinary Essential Questions and Perspectives for Teaching and Learning Chemistry*, 33 SCI. & EDUC. 1503 (2023)(chemistry); Sheila Scott, *Repetitions and Contrasts: Using Essential Questions to Frame Unit Plans in General Music*, 27 GENERAL MUSIC TODAY 22 (2014)(music).

[15] Jeffrey D. Wilhelm, *Learning to Love the Questions: How Essential Questions Promote Creativity and Deep Learning*, 42 KNOWLEDGE QUEST 36, 41 (2014).

[16] *Id.* at 38.

> extend further learning and to solve problems in students' lives and out in the world."[17]

In other words, EQTS creates lifelong learners, not simply course completers. This mirrors Professor Ken Bain's research on what the best college teachers do.[18] For Bain, the best college instructors are those that follow the liberal arts tradition.[19] This means that the courses not only focus upon substantive course topics, but also incorporate critical thinking, problem solving, creativity, and curiosity.[20] The best teachers design courses to teach "students to understand, analyze, synthesize, and evaluate evidence and conclusions."[21] In other words, the best teachers avoid content regurgitation and strategize to develop the critical thinking and problem-solving abilities of their students. This is a pedagogical challenge because student academic strategies are often different from those professors want students to use. Students often adopt academic strategies that "control college."[22] Students see controlling college as being able to (1) shape their own schedules, (2) tame professors, and (3) limit course workloads.[23]

EQTS is a means to meet Bain's description of the best teacher, develop life-long learners, and reduce the likelihood that students are simply taming the professor. It centralizes both content mastery and critical thinking development.[24] Using EQTS means student thinking is centralized, i.e. teachers think about the way that students think.[25] In the liberal arts tradition, the strategy can also help develop critical engagement skills that are:

> "Needed in our democratic citizenry: a willingness to examine multiple perspectives, ask thoughtful questions, seek out additional information, debate ideas with peers, consider the causes and potential consequences of actions, and re-consider our own opinions and understanding in light of new evidence and alternative analyses."[26]

Further, EQTS is an important tool to develop and maintain student engagement. Student engagement is found to contribute to both better academic performance and individual well-being.[27] EQTS utilizes four types of questions. Used purposefully, the questions engage students in course concepts and topics and encourage continued exploration. The essential question is the

[17] *Id.* at 41.
[18] KEN BAIN, WHAT THE BEST COLLEGE TEACHERS DO, 7 (2004).
[19] *Id.* at 8.
[20] *Id.*
[21] *Id.* at 8-9 & 115.
[22] Danes-Staples, *supra* note 12 (citing Rebekah Nathan, MY FRESHMAN YEAR: WHAT A PROFESSOR LEARNED BY BECOMING A STUDENT, 115-16 (2006)).
[23] *Id.*
[24] Virgin, *supra* note 14, at 202 (2014); Doug Lillydahl, *Questioning Questioning: Essential Questions in English Classrooms*, ENGLISH J. 36, 37 (2015)("Students need to see classroom connection to their lives and interests, and while some of our students are deeply motivated by skills inquiry, many others feel skills are fatally tainted by practicality and challenge.").
[25] Virgin, *supra* note 14, at 201; Lattimer, *supra* note 14, at 326.
[26] *Id.* at 327.
[27] Matthew J. Bundick et. al., *Promoting Student Engagement in the Classroom*, 116 TEACHERS COLL. RECORD 040302, 4-5 (2014)(aggregating student engagement research and providing teaching strategies to increase student engagement).

principal component of EQTS and receives support from hype, leading, and guiding questions. The following sections explore each type of question in further detail.

A. The Essential Question

1. The Purpose and Characteristics of an Essential Question

The principal component of EQTS's is the essential question. The essential question helps frame either an entire course or a specific course topic.[28] Further, the essential question is transferable, meaning it be applied across disciplines, across the major, or across topics covered in a particular course.[29] The question helps students work through seemingly abstract, disconnected concepts that experts, through experience and gained knowledge, may find simple.[30] Students use important concepts to initially answer an essential question and, then, continue to examine the essential question to develop a more complete answer.[31] Even when students offer an initial response, an essential question is re-asked to deepen understanding.[32] This understanding provides a broader context across course topics, avoiding isolated learning outcomes.[33] As thought is stimulated, students raise even more questions related to the introduced essential question.[34]

McTighe & Wiggins state that essential questions contain most, if not all the following characteristics (some covered previously and listed comprehensively here):

1) Open-ended,
2) Thought provoking or intellectually engaging,
3) Seeks higher-order thinking,
4) Points towards transferable ideas,
5) Raises additional questions,
6) Requires support and justification, and
7) Can be revisited repeatedly in the course or broader curriculum."[35]

Ostensen & Gleason-Sutton add that an essential question provides students with the opportunity to connect with their own experiences and perspectives.[36] Due to technological developments, today's students "are members of participatory cultures created with social technologies that emphasize collaboration, information sharing, and networking."[37] The nature of essential questions requires an instructor, or course designer, to consider what they want such students to explore and take away from the course. It also requires instructors to consider what students think about, or would consider, in relation to the course content. Examples of essential

[28] Jay McTighe & Grant Wiggins, ESSENTIAL QUESTIONS: OPENING DOORS TO STUDENT UNDERSTANDING, 9 (2013).
[29] *Id.* at 9.
[30] *Id*. at 4.
[31] *Id.* at 9.
[32] *Id.* at 14 & 16.
[33] Lillydahl, *supra* note 14, at 37.
[34] McTighe & Wiggins, *supra* note 28, at 3.
[35] McTighe & Wiggins, *supra* note 28, at 3.
[36] Jonathan Ostensen & Elizabeth Gleason-Sutton, *Making the Classics Matter to Students through Digital Literacies and Essential Questions*, 101 ENGLISH J. 37 (2011).
[37] Karen Brown, *Questions for the 21st-Century Learner*, 38 KNOWLEDGE QUEST 24, 25 (2009).

questions across disciplines help clarify the characteristics. The following section explores the use of essential questions in other disciplines.

2. Essential Questions in Other Disciplines

Other academic disciplines have used EQTS. Wilhelm lists essential questions for a number of disciplines.[38] For example, in literature, an essential question framed lessons concerning the novel *The Scarlet Letter*.[39] Ostenson & Gleason-Sutton refer to the novel as "the bane of many of our high school students' existence."[40] However, creating lessons with EQTS gave the novel "real meaning for our students."[41] The essential question framing *The Scarlet Letter* was "What is worth risking everything for?"[42] The question serves two functions: (1) it connects to a central theme of the novel and (2) it connects to something students already experience, i.e. evaluating risk.[43] Then, classroom activities were designed around the essential question concerning risk. Some activities preceded discussions of the novel, attempting to have students think about firsthand experiences with risk.[44] Using the essential question gave instructors the ability to focus upon portions of the novel that connected more to students, allowing students to point out parts of the novel where they identified a character taking or contemplating risk.[45]

Lessons in history provide illuminating examples of essential questions. History instructors use essential questions to "address the contested concepts and dilemmas that historians puzzle over in their work" and "require students and teachers to view the content from multiple perspectives."[46] Lattimer provides an example used to historically explore the essential question, "Should there be limits on personal freedom?"[47] A class would begin by connecting with students where they are, or as Lattimer describes it, building on student experiences with "dress codes, curfews, drivers' license restrictions, and legal alcohol and drug use."[48] Students were asked to rank, 1-10, each restriction's appropriateness and then defend their position.[49] The defenses, and other student responses, raised additional questions explored throughout the lesson and were then applied to primary source case studies about personal freedom.[50] The result was that students "began to conceptualize their study of the past more critically," questioning their own initial positions and raising further questions to explore.[51]

In mathematics, essential questions add instructional value because they "are applicable to a wide range of problem-solving tasks and do not prescribe specific mathematical steps for solving a particular type of problem."[52] Kress created essential questions to help students see the problem

[38] Wilhelm, *supra* note 15.
[39] Ostensen & Gleason-Sutton, *supra* note 36.
[40] *Id.* at 37.
[41] *Id.*
[42] *Id.* at 38.
[43] *Id.*
[44] *Id.* at 38-9.
[45] *Id.* at 39.
[46] Lattimer, *supra* note 14, at 326.
[47] *Id.* at 327.
[48] *Id.*
[49] *Id.*
[50] *Id.* at 328 (stating that the lessons chosen revolved around the changing roles of women in the United States, the prohibition of alcohol in the 1920s, and the rise of the Ku Klux Klan and expressions of racism).
[51] *Id.* at 329.
[52] Kress *supra* note 14, at 192.

before them, to clarify confusion, and to identify missing or additional information. For example, In the place of "detailed procedural instructions" to solve a problem, Kress presents the following questions to students: (1) "What do you notice?", (2) "What can you do to figure it out?", (3) "How do you know that your work and answer are accurate?", (4) Is there another way you could approach this problem?", and (5) "What else can you say about the problem, and what else would you like to know?"[53] These questions provide structure to students while giving them the opportunity to "recognize and take ownership of the actions underlying their success."[54]

In 2014, Jeffery Wilhelm proposed the following essential question under the topic of cultural issues but illustrates its usefulness in the sport management curriculum: "Are sports (or competition) overemphasized in North American culture?"[55] This may not be a question specifically applicable in sports law but does illustrate how essential questions may be developed for the sports law and, more broadly, the sports management curriculum.

Once an essential question is chosen, instructors must think about and plan to use other types of questions to gain, develop, and hold student interest. The following section discusses those other questions and how they support the essential question.

3. Other Questions that Support the Essential Questions

The article concludes by offering essential questions related to DeMartini& Kao's findings of the most important sports law topics - Title IX and torts. But, before that section, it is important to generally introduce other question types that serve important pedagogical purposes. Those purposes include (1) initiating interest in a subject, (2) sustaining attention in the subject, and (3) guiding students towards understanding and exploring the essential questions posed. Those questions are hype, leading, and guiding questions. The following three sections explain each.

a. Hype Questions

To introduce a subject, an initial style of question is the hype question. Hype questions have limited utility but are critical for attracting student interest.[56] Referred to as the match that starts a fire, the hype question helps hook students on the topic.[57] The hype question is an attempt to meet students where they are while beginning the introduction to an important legal topic. Hype questions draw out responses, initiating what can develop into a deeper conversation. A couple of examples include: (1) to open a discussion about laws that affect employment, a professor might ask "Who has been paid by the hour and do you mind sharing how much?" having students share a personal experience that, whether they are aware or not, is directly connected to statutory law; or (2) to open a discussion about criminal procedure, an instructor may ask, "You don't have to answer if you do not wish to, but has anyone experienced being pulled over by a police officer?"

Although current students are collaborative through social media,[58] it is often difficult to generate open classroom interaction. A student's comfort in a particular classroom setting may

[53] *Id.,* at 193-94 & 196.
[54] *Id.* at 196.
[55] Wilhelm, *supra* note 15, at 39.
[56] McTighe & Wiggins, *supra* note 28, at 12.
[57] *Id.*
[58] Brown *supra* note 37, at 25.

influence the willingness or reluctance to participate in classroom discussions.[59] Thus, professors must choose the types of hype questions, as well as the methods of introducing the questions, with consideration as to whether the hype question will succeed in generating class responses and discussion. To jump-start classroom discussion, two methods to introduce hype questions include small group discussions[60] and classroom polling.[61] Once hype questions are introduced, and a discussion begins, it is important for the instructor to keep students on the path towards learning objectives – to lead students along. The following section covers the use of leading questions in context of EQTS.

b. Leading Questions

Once hype questions attract student attention, leading questions are used to begin the deeper dive into legal principles, statutes, and other valuable information important to student learning. Laws and legal opinions are specific and do require detailed understanding of their practical application. The rhetorical nature of a leading question directs students towards that practicality.[62] By answering leading questions, students learn contextual knowledge and begin to apply that knowledge to varying scenarios. For example, following the hype question about students being pulled over by a police officer, a leading question may broadly ask, "Where can we find rules, laws, and information about how police officers are to pull over drivers?" or, another way, "What reasons are police officers allowed to pull over a driver and begin to interact with the driver?" The leading questions begin the exploration into the basic procedures for police officer interaction.

More specific to the sports law curriculum, referring again to facilities management, an example of a leading question is, "Are there required safety measures for sporting events?" This question can be broken down further into various categories as well, i.e., event access, spectator safety, emergency procedures, food and beverage safety requirements, employee protections, and potentially others. This provides an excellent opportunity for small group activities to discover the law's effect upon these areas of facilities management. This could also lead to class projects/presentations as students build research based upon the leading question.

Leading questions do have limits. Too many leading questions can overwhelm students and move them towards rote memorization – a hinderance to critical thinking development.[63] So, EQTS requires the right number of leading questions so that students gain practical knowledge to enhance the class conversation but are not simply memorizing for a test or assignment. Instructors should take the time to consider what questions should lead students to learn and when leading questions should stop so students are able to focus within the topic.

Leading questions help build concrete knowledge which then allows the introduction of broader ideas about the law and the law's application. This means turning to guiding questions to

[59] Crystena Parker-Shandel, *Participation in Higher Education Classroom Discussions: How Students' Identities Influence Perspective Taking and Engagement*, 11 TEACHING & LEARNING INQUIRY 1, 14 (2019).
[60] *Id.*
[61] Joss Ives et. al., *Requiring Mobile Devices in the Classroom: The Use of Web-based Polling Does Not Lead to Increased Levels of Distraction*, 7 J. STEM EDUC. RESEARCH 307, 318 (2024)(finding that active classroom participation in polling activities decreases student distraction when compared to passive classroom participation).
[62] McTighe & Wiggins, *supra* note 28, at 11.
[63] Jennifer S. Anderson, et al., *Insights from Snowboard Pedagogy for Legal Studies Instructors*, 16 DEPAUL J. SPORTS L. 225, 225 (2020).

build student insight and confidence with the materials. Guiding questions are explained in the following section.

c. Guiding Questions

Similar to leading questions, guiding questions focus on a specific conclusion or outcome, like how a law applies to a particular fact pattern.[64] However, guiding questions are broader in scope requiring more than simple recall.[65] The questions are not intended to be revisited throughout a course, but address a particular class topic.[66] They are not intended to be explored throughout the course, but to help students reach conclusions about the topic before them.[67]

For example, within the topic of facility management, a guiding question may be "Should a baseball organization be responsible for a fan's injury caused by a foul ball?" This guiding question will generate more questions – more *what ifs*. The *what ifs* might include: "What if the fan is reaching onto the field?", "What if the fan is not paying attention to the game?", "What if there is a hole in the safety netting?", and "What if the ball does not directly hit the fan, but ricochets and eventually hits the fan?" The questions serve two purposes. One, if students begin to offer what if questions, they are engaged in learning.

In law, using guiding questions provides a way for students to understand what I refer to as the *what ifs* – the changes in fact patterns that could create changes in the legal outcome. Students presented with one fact pattern, and one legal conclusion, will often change a fact and ask whether the legal outcome would change. They often begin these questions with "What if…" I encourage instructors to turn those *what ifs* into guiding questions where students research and find answers to the *what ifs* they raise. Now that EQTS and its components are generally covered, section III turns to applying EQTS in the sports law curriculum.

III. ESSENTIAL QUESTIONS IN SPORTS LAW: TITLE IX & NEGLIGENCE

Sports Law instructors routinely emphasize the value of both critical thinking and problem-solving skills.[68] Developing course materials with EQTS helps accomplish this objective. It is a particularly useful strategy in law because course questions can be generated from real-world cases.[69] The sections below provide sample essential question lessons to adopt, adapt, and improve upon. Because De Martini & Kao found Title IX and negligence the most common subjects covered in the sports law curriculum, the following sections provide essential questions lessons for those topics, respectively. Section A's focus is on two areas of Title IX. Section B focuses on negligence.

[64] McTighe & Wiggins, *supra* note 28, at 11.
[65] *Id.*
[66] *Id.* at 11-12.
[67] *Id.* at 12.
[68] Braunstein-Minkove *supra* note 8, at 136.
[69] *See* Karen E. Spierling, *College is the Real World*, INSIDE HIGHER EDUC., Apr. 6, 2023, https://www.insidehighered.com/views/2023/04/06/dont-buy-myth-college-real-world-opinion (challenging the argument that college courses and campus life are somehow disconnected from the "real world.").

A. Essential Questions for Title IX

The following sections present the EQTS to help students understand two areas of Title IX – equal opportunity and gender harassment/violence. The focus in this section is upon the questions instructors may use to generate class discussion and potential assignments. Appendix A provides a table summarizing the following two sections. The table may be used as a guide to adopt Title IX into the sports law curriculum.

1. Equal Opportunity: What Makes an Equitable Sports Environment?

Teaching sports law students Title IX offers an ideal opportunity to utilize EQTS. Professor Adam Epstein's 2013 work developing the Sports Law curriculum provides a starting point.[70] Professor Epstein suggests opening the topic of Title IX by asking the students "What is equity?"[71] Then, Epstein suggests following up with two other questions: "Is equity the same as equality?"," Is equity the same as equitable?"[72] As essential questions, each question Professor Epstein suggests is too generic but on the right track.[73] Professor Epstein's questions help to develop an essential question for a lesson in Title IX.

Keeping in mind the characteristics of a quality essential question and taking the liberty of editing Professor Epstein's opening questions, an essential Title IX question for equal opportunity is: "*What does it take to create equal opportunity in sport?"* or, another way, "*What makes an equitable sports environment?"* This question is open-ended, presents an intellectually intriguing problem the class will revisit throughout the lesson, raises additional questions, and requires support and justification as students explore and present answers. With this question, students have a starting point from which an exploration and understanding of Title IX might begin.

But teachers will need to draw students into the topic and then guide them through the foundational knowledge necessary to discuss the essential question posed. Drawing students in - capturing their attention - means using a hype question. Teachers can generate hype questions from news or case law. Or hype may directly connect with students where they are with only indirect connection to the topic. In the case of Title IX, an indirect hype question might be, "Would it be acceptable to organize this class with one group of students always assigned to the front of the class and another group of students assigned to the back of the class?" Another could address classroom resources: "What if we gave only the female students advanced artificial intelligence tools to complete the coursework?" The answers to these questions will revolve around fairness, justice, and equity. Further, "What if male students could only take this class at 8:00 am 5 times a week, while female students had the opportunity to choose between 4 different course start times that met only twice a week?"

It is important to recognize that presenting the hype question may result in strong opposing opinions, especially in relation to gender equity.[74] Plus, some students find gender issues

[70] Adam Epstein, *The Fundamentals of Teaching Sports Law*, 4 WILLAMETTE SPORTS L. J. 1, 17 (2013).
[71] *Id.*
[72] *Id.*
[73] Wilhelm, *supra* note 15, at 40-41.
[74] Josie Cox, *Gen Z Has a Big Gender Gap When It Comes to Views on Feminism, Study Shows*, FORBES.COM, Mar. 6, 2025, https://www.forbes.com/sites/josiecox/2025/03/06/gen-z-has-a-big-gender-gap-when-it-comes-to-views-on-feminism/.

emotionally challenging, and preparation will be required to address those challenges.[75] But covering Title IX effectively means working with various opinions and views about gender equity to gain a useful, shared understanding of the law and, ultimately, to learn to create corporate (university) policy and strategy within the guidelines of Title IX. Well-planned introductions to Title IX within EQTS, using well thought-out hype questions, creates a platform to do so.

With interest sparked, utilizing leading questions helps students understand Title IX and its purpose. A leading question might be, "How are fairness and equity addressed in Title IX?" This requires finding specific responses through research. Students might conduct research in groups during class time or outside of class for discussion in the following meeting. A leading question might connect the hype question to sport. "How might equity in sport be similar to equity in the classroom?" This helps students understand Title IX applies across all educational opportunities, including sports opportunities.[76]

Using another leading question helps students consider exceptions to Title IX: "What if the school is discriminating based upon its religious foundations? What is the Title IX analysis?" This is a small but important distinction in the law that begins an exploration of legal exemptions.[77]

Additional leading questions might be: "Does equity mean providing the same sports, the same funding, or the same facilities?", "Does equity mean that male and female opportunities are completely equal across all sports or only within the same sport?" "How might name, image, and likeness opportunities fit with equity?" The questions all provide the opportunity for research during class, as preparation for the following class, or as a student presentation.

Guiding questions work similarly. These can be based upon actual case law or other legal resources, guiding students towards the resources needed to be informed managers. For example, a letter from the U.S. Department of Education Office of Civil Rights to the University of Mount Olive concerning a disparity in facilities for softball (women's sport) and baseball (men's sport) helps create this: "Under Title IX, how similar do athletics facilities have to be?"[78]

Radwan v. Manuel[79] provides another equal opportunity fact pattern that can be explored with EQTS. In *Radwan*, a female soccer player at the University of Connecticut (UConn), while celebrating a close win, looked directly at an on-field camera and stuck up her middle finger.[80] The player lost her place on the team and her full scholarship as punishment for the gesture.[81] As the Second Circuit pointed out, under the athletic director's tenure at UConn, "no male student-athlete was ever permanently removed from his team, or had his scholarship terminated, for a first instance of unsportsmanlike conduct."[82]

[75] Shawna Eikenberry & April Sellers, *Teaching Issues of Equity and Oppression in a Business Ethics Course*, 21 J. SCHOLARSHIP TEACHING LEARNING 121, 121 & 130 (2021).
[76] 20 U.S.C. § 1681(a)("No person in the United States shall, on the basis of sex, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any education program or activity receiving federal financial assistance."); Oldham v. Pa. State Univ., 2025 U.S. App LEXIS 13067, *19 (3rd Cir. 2025)("Thus, Title IX covers the operations of colleges and universities that may be reasonably considered, at least in part, educational.")
[77] 20 U.S.C. § 1681(a)(3)(exempting religious institutions "with contrary religious tenets.").
[78] United States Department of Education Office of Civil Rights, *Letter to University of Mount Olive*, Case No. 11-24-2150, 2 (July 19, 2024)(outlining the factors used to determined Title IX compliance in athletics facilities and finding the University of Mount Olive out of compliance when comparing softball and baseball).
[79] 55 F.4th 101 (2d Cir. 2022).
[80] Radwan v. Univ. of Conn. Bd. of Trs., 464 F. Supp 3d 75, 84-85 (D.Conn. 2020).
[81] 55 F.4th at 105.
[82] *Id.* at 135.

Instructors may introduce guiding questions like, "Taking Radwan as an example, in what other ways might student-athletes be treated differently?", "In what ways might student-athletes treatment be different because of the student-athlete's gender?", and "How might athletic department leaders implement programs or safeguards to avoid equal opportunity violations?" These final questions, of course, provide further opportunity for research, projects, presentations, and other forms of work an instructor may choose to include.

2. Gender Harassment/Violence: How Can a University Protect the Physical/Emotional Well-Being of Its Students?

Title IX also includes protections for individuals treated differently or violently in relation to their sex – both considered forms of discrimination.[83] An essential question to frame this area of Title IX could be: "*How can a university protect the physical/emotional well-being of its students?*"[84]

A hype question brings the conversation close to student experience: "What reasons do students fail or drop out of college courses?" This question is broad, and many answers may have nothing to do with Title IX coverage. Patience will reveal that eventually students will offer traumatic or difficult events as reasons to drop out of or fail a college course. Leading questions can then bring Title IX into the conversation: "Do people experience trauma or difficulty because of their gender?" Students, of any gender, can provide stories about themselves or others who may have experienced gender-related trauma. The conversation may provide unique stories or responses for the instructor to take note of and possibly use as the discussion continues.

The next leading question brings us closer to the requirements of Title IX but allows students to consider it before reaching that concrete answer. The question is: "Does gender-related trauma or difficulty lead to academic difficulties?" The question, and its responses, are evidence-based.[85] A follow-up leading question will get closer to the purpose of Title IX – "How are colleges and universities expected to prevent and respond to sexual harassment and violence on campus?" The available materials addressing this question is a candidate for a research assignment, in or out of class.

Guiding questions then, can delve into the law in more detail. The guiding questions should help students see (1) how university policy is created to comply with Title IX, potentially preventing sexual violence, (2) how universities fail to prevent or respond to sexual violence (i.e., comply with Title IX, and (3) legal reactions to university failures to comply or affirmations of compliance (mainly through court decisions). Some guiding, researchable questions might include: (1) Who should be aware of and be required to prevent gender-related harassment and violence?,

[83] *Title IX and Sex Discrimination,* U.S. DEPT. OF EDUC. (last visited Jun. 6, 2025)(stating that discrimination as defined under Title IX includes "sex-based harassment" and "sexual violence").

[84] This question is supported by research. *See* Carol E. Jordan, et al., *An Exploration of Sexual Victimization and Academic Performance Among College Women*, 15 TRAUMA, VIOLENCE, & ABUSE 191, 196 (2014); Cecilia Mengo & Beverly M. Black, *Violence Victimization on a College Campus: Impact on GPA and School Dropout*, 18 J. COLL. STUDENT RETENTION: RESEARCH, THEORY & PRACTICE 234,235 (2015)(explaining the multiple negative consequences victims of sexual violence may experience).

[85] Taylor D. Molstad, et al., *Sexual Assault as a Contributor to Academic Outcomes in University: A System Review*, 24 TRAUMA, VIOLENCE, & ABUSE 218, 227(2023)(performing a systemic review of relevant literature and finding that "Across the studies in the review, there was a consensus among findings that victims of sexual assault suffer academic outcomes.")

(2) How might a university prevent gender-related harassment and violence?, or (3) Are there best practices that universities should adopt?

B. An Essential Question in Negligence: What Reasons Might One Be Responsible For the Safety and Well-Being of Others?

This section presents a way to use EQTS to help students understand negligence. The focus here is upon the types of questions to generate discussion and potential assignments. Appendix B provides a framework to use EQTS while covering negligence.

Covering negligence in the sports law curriculum trains students to answer an important strategic question. Negligence requires identifying responsibility for the safety and well-being of others, including for sports organizations.[86] Written as an essential question, this standard would be: *What reasons are we responsible for the safety and well-being of others?* Generalizing the questions with "we" provides students the opportunity to determine what person, persons, or organizations can replace "we" in the question. Students may come up with multiple entities that may be responsible. Following the identification of a responsible entity, students can develop reasons for responsibility.

To put this in negligence language, exploring this essential question engages students with the first element of a negligence evaluation – identifying whether a duty to others exists.[87] To reach the essential question, hype, leading and guiding questions are used to develop the lesson around negligent liability. As a quick aside, hype and leading questions do not necessarily have to be about sports. They can be broader in scope to have students generate responses showing they have critically considered the questions. The guiding questions then incorporate sports more specifically.

Three different topics will be used here to create hype, leading, and guiding questions. But instructors are encouraged to create questions using a topic best suited to their make-up of students and student interests. Driving and wrecks are a topic generally applicable to all classes I teach – although in a populated city this may not apply. A hype question for this topic is simply: *Who has or knows someone who has experienced a car wreck?* Students are usually engaged in this discussion, because driving and car crashes are such common occurrences. Once students offer that they have, or they know someone who has, the instructor can hype further by asking about fault – using the Socratic method to delve into whether a student's fault analysis is accurate. The time of year may also influence which topic to choose. Around Halloween, I create hype, leading, and guiding questions around haunted houses to discuss the essential question of responsibility for injuries.

[86] *See* Sam C. Ehrlich, *Swimming Against the Current: Mayall v. USA Water Polo and Its Potential Impact on Overseeing Athletic Organizations*, 19 VA. SPORTS & ENT. L. J. 1 (2019)(reviewing a 2019 Ninth Circuit decision for its impact upon amateur sports organizations potential negligence liability); *see also* Sam C. Ehrlich, *Gratuitous Promises: Overseeing Athletic Organizations and the Duty of Care*, 25 JEFFREY S. MOORAD SPORTS L. J. 1 (2018)(discussing negligence liability for sports organizations through analysis of six other cases).

[87] Lares v, Doe, 2025 Mich. App. LEXIS 2382, *7 (Mich. App. 2025)(recreational referees owe duty to participants not to act recklessly); Limones v. Sch. Dist. 161 So. 3d 384, 389 (FL 2015)(secondary school personnel has duty to protect and sometimes act to protect student athletes); Regents of Univ. of Cal. v. Superior Ct., 29 Cal.App. 5th 607, 625-27(CA App. 2018)(a college's special relationship with enrolled students creates duty to maintain safe campus environment) ; Avila v. Citrus Comm. Coll. Dist., 38 Cal. 4th 148, 158 (2006)(colleges owe duty of care to their athletes);

Following a general discussion of legal fault, a leading question helps the focus turn towards a legal evaluation. The question could be: "Does it make sense that the law sometimes holds the driver at fault and sometimes does not?" After a discussion of this question, the following leading question broadens the conversation: "In what other types of sports-related situations does the law impose fault, responsibility?" Students will generate several responses that bring forth the various relationships involved in sports-related injuries.

The guiding questions then provide the opportunity to connect negligence to sport. An example of a guiding question to focus upon sports might be: "Within sports, how is fault applied when someone is injured?" The question offers the opportunity for student research and discovery. Instructors may then choose assignments/classroom activities that encourage this research and discovery – both in and outside of class meeting times. The guiding question may be, for example, introduced while students are working in small groups, allowing each group to develop its own research and responses.

When introducing the negligence-focused EQ to students, connecting to students through events or experiences close to them is important. Using home football or basketball games provides a great environment to discuss potential liability issues. Most students who choose to attend a university with a football team are aware of the home game environment. Hype, leading, and guiding questions can be developed using this sporting environment.

To be even more specific, a discussion could focus upon one unique to sports - field storming.[88] Fans storm the playing field or court after their team wins. This chaotic environment raises significant liability concerns. Universities and conferences continue to grapple with ways to reduce field storming incidents.[89] Using field storming is a great way to develop an essential questions conversation or course assignments. The following paragraphs build a essential questions lesson using field storming.

As a hype question, ask the class, "Has anyone stormed a field or court after a game?" If they have not done so themselves, ask if they have seen it on television. If not still, an internet search will quickly find videos to demonstrate the event. Once students understand what it is, a leading question helps begin to discuss the possible negative consequences – "Is it possible for people to be injured when storming the field?" This can be followed with guiding questions that address who or what may be hurt (as negligence covers both persons and property) and in what ways? Small group discussions can be used to have students list the types of people or property that can be injured as well as the ways that injuries might occur.

Once types of injuries and categories of persons/property are developed, a further leading question helps students think about negligent responsibility: "To which persons/property does the home university owe protection from potential injury?" This question provides students with the opportunity to see both the inclusions and limitations of negligent liability.

Finally, guiding questions help students strategically consider solutions to limit field storming liability. The guiding questions might include: "How might a university develop policies to reduce field storming?", "In what ways might a university control field access to reduce field storming?", "Is it possible to include in stadium design protections against field storming?", "What

[88] KTO, *The Chaotic History of "Storming the Field,"* YOUTUBE.COM, https://www.youtube.com/watch?v=YEbLPECYhEA&ab_channel=KTO (providing a montage of videos of field storming in college football).

[89] *See* Associated Press, *SEC Increases Fines to $ 500K for Storming Field, Court*, ESPN.COM, May 29, 2025, https://www.espn.com/college-football/story/_/id/45380660/sec-increases-fines-500k-rushing-field-court; *see also* Reggie Anderson, *ACC Unveils New Policy Concerning Storming Field, Courts*, WCNC.COM, Jul. 23, 2025, https://www.wcnc.com/article/sports/ncaa/acc-fan-policy/101-16b7b9c6-a58e-4505-866e-5b79e913e929.

about ticketing language? Can this be used to reduce liability in these situations?" Instructors may develop in-class or homework assignments related to this topic, including case and news research to show students this is a concern in the real world. Finally, instructors may ask students to think about other environments, either on campus or off, where potential for injury requires strategic thought and action. This guiding question broadens the liability concept beyond field storming so that students begin to realize that similar legal questions – especially those involving negligent liability – are important strategic considerations in multiple business settings.

IV. CONCLUSION

This article introduces the essential questions teaching strategy for the sports law curriculum. Instructors in sports law, and sports management more generally, value development of both hard and soft skills. EQTS allows students engage with course concepts while simultaneously developing the critical thinking skills necessary to solve complex problems – objectives in the sport management curricula and in sports law courses. The article covered EQTS and its components, generally, and then offered two sports law specific examples of EQTS – Title IX and negligence – chosen based upon research into the most commonly covered topics in the sports law curriculum. Using EQTS provides the sports law instructor with the framework to take important topics, build student interest and engagement, and enhance student understanding of complex legal issues. I hope this article sparks an interest in doing so.

APPENDIX A
TABLE 1

ESSENTIAL QUESTIONS FOR TITLE IX (EQUAL OPPORTUNITY)

The table below provides EQTS examples for the Title IX subcategory equal opportunity. It is not intended to be exhaustive as Title IX case law is expansive. Instructors may choose to follow student responses and research, to build upon the questions posed below.

TOPIC	ESSENTIAL QUESTION	HYPE QUESTIONS	LEADING QUESTIONS	GUIDING QUESTIONS
Title IX: Equal Opportunity	*What makes an equitable sports environment?*	*Would it be acceptable to organize this class with one group of students always assigned to the front of the class and another group of students assigned to the back of the class?* *What if we gave only the female students advanced artificial intelligence tools to complete the coursework?*	*Does equity mean providing the same sports, the same funding, or the same facilities?* *Does equity mean that male and female opportunities are completely equal across all sports or only within the same sport?* *How might name, image, and likeness opportunities fit with equity?*	*How do colleges evaluate equal opportunity for Title IX compliance?* *Under Title IX guidance, how similar must athletics facilities be?* *Under Title IX guidance, how similar must athletics benefits be (clothing, NIL assistance, tournaments, etc)?*

Title IX: Equal Opportunity Cases/Resources

Myers v. Stephen F. Austin State Univ., 2025 U.S. Dist. LEXIS 151615 (E.D. Tex. 2025)
- Female athletes sue following university's elimination of some female sports.
- In preliminary injunction evaluation, the district court works through the three prongs of Title IX's equal opportunity analysis.

Radwan v. Manuel, 55 4th 101 (2d, Cir. 2022)
- Female college athlete proves she was punished more harshly than male college athletes for similar behavior.

U.S. Dept. of Education, Office of Civil Rights, Letter to University of Mount Olive, Jul. 19, 2024.
- Comparing the university's softball and baseball facilities for gender disparities.[90]

[90] https://ocrcas.ed.gov/sites/default/files/ocr-letters-and-agreements/11242150-a.pdf

APPENDIX A
TABLE 2

TITLE IX ESSENTIAL QUESTIONS - GENDER HARASSMENT/VIOLENCE

The table below provides EQTS examples for Title IX gender harassment/violence coverage. Cases are provided to connect the classroom work to the real world. This table is not intended to be exhaustive as Title IX case law is expansive. Instructors may prefer other sources. While using EQTS, instructors may also choose to follow student responses, or student research, to arrive at an understanding of the essential question.

Gender harassment/violence is an important topic to cover in relation to Title IX. But the fact patterns and discussion of the legal issues may be difficult for some students. Instructors are encouraged to take great care in preparation and delivery of this topic.

TOPIC	ESSENTIAL QUESTION	HYPE QUESTIONS	LEADING QUESTIONS	GUIDING QUESTIONS
Title IX: Gender Harassment/Violence	*How can a university protect the physical/emotional well-being of its students?*	*Do you know someone who is struggling academically?* *What reasons do students fail or drop out of college courses?*	*Do people experience trauma or difficulty because of their gender?* *Does gender-related trauma or difficulty lead to academic or athletic difficulties?* *How are colleges and universities expected to prevent and respond to sexual harassment and violence on campus?*	*Who should be aware of and be required to prevent gender-related harassment and violence?* *How might a university prevent gender-related harassment and violence?* *Are there best practices that universities should adopt?*

Title IX: Sexual Harassment/Violence Cases

Instructor's Note: The included case fact patterns require strong discernment when deciding to include or exclude from a particular class. Instructors should read these cases carefully to determine the appropriateness for their respective students.

Arana v. Bd. of Regents v. Univ. of Wis. Sys., 2025 U.S. App. LEXIS 17180 (2025)

- University Title IX liability to victim after readmitting a star football player found responsible for sexual assault and harassment by the university but not guilty at trial.

Doe v. Ohio Univ., 2023 U.S. Dist. LEXIS 52435 (S.D. Oh. 2023)

- Deliberate indifference to harassment and gender discrimination during hearing proceedings.

Kollaritsch v. Mich. State Univ. Bd. of Trs., 944 F.3d 616 (6th Cir. 2019)

- Analyzing the legal definition of sexual harassment when victim continues to encounter perpetrator on campus.

Oldham v. Pennsylvania St. Univ., 138 F. 4th 731 (3rd Cir. 2025)

- The "zone of interest" case to determine what victims are covered by Title IX.

Owens v. Louisiana State University, 709 F. Supp. 3d 219 (M.D. La. 2023)

- Electronic communication with victim following a sexual violence incident.
- News article concerning the case:
    - Andrea Gallo, *New Derrius Guice Rape Allegations Emerge in Updated Lawsuit About LSU Sexual Misconduct*, THE ADVOCATE, Jun. 25, 2021 https://www.theadvocate.com/baton_rouge/news/education/new-derrius-guice-rape-allegations-emerge-in-updated-lawsuit-about-lsu-sexual-misconduct/article_8539f3f8-d5e6-11eb-98a8-93ca1ca76c54.html

Roe v. Marshall Univ. Bd. of Governors, 2025 U.S. App. LEXIS 19213 (4th Cir. 2025)

- Differentiating on-campus and off-campus incidents in relation to university Title IX liability.

APPENDIX B
ESSENTIAL QUESTIONS FOR NEGLIGENCE

This table provides EQTS examples for negligence. A list of cases is provided as real-world examples to support EQTS. Neither are intended to be exhaustive. Using certain cases might be appropriate given the time of year negligence is discussed. If it is football season, a case involving football players or fans may attract student attention. In October, or the first week of November, cases that involve a haunted house works well. Other examples are not tied to a particular time of year, such as those concerning car accidents or injuries on a college campus. No matter the case, EQTS is used to drive student engagement, conversation, and ultimately understanding.

TOPIC	ESSENTIAL QUESTION	HYPE QUESTIONS	LEADING QUESTIONS	GUIDING QUESTIONS
Negligence	*What reasons might someone be responsible for the safety and well-being of others?*	*Who in the class has experienced a car wreck?* *Who likes haunted houses?* *How safe is your campus environment (dorm room, walkways, campus access, school activities, etc.)?* *Have you been at a concert or sporting event where conditions were dangerous?*	*How do we know who is responsible when a car wreck happens?* *How might injuries occur when experiencing a haunted house?* *Does a university have a responsibility to fix unsafe environments?* *Does a university have a responsibility to warn of unsafe issues or people?* *What types of events require special attention to safety?*	*What steps or strategies might be used to avoid responsibility when a car wreck happens?* *Within sports, how is fault applied when someone is injured?* *What strategies might be implemented to prevent injuries* *What strategies might a university take to create a safe environment for students? For employees? For those not associated with the university?* *Are there best practices to avoid injuries around sports events?*

Sport-Related Negligence Cases

Avila v. Citrus Community Coll. Dist., 38 Cal. 4th 148 (CA 2006)
- University liability for an intentional baseball pitch that injured the batter.

Davidson v. Univ. of N.C. at Chapel Hill, 142 NC App. 544 (NC App. 2001)
- Duty to JV cheerleading squad in relation to safe participation.

Kleinknecht v. Gettysburg Coll.,989 F. 2d 1360 (3rd Cir. 1993)
- Duty of college in relation to lacrosse player's death during practice.

Lares v. Doe, 2025 Mich. App. LEXIS 2382 (Mich. App. 2025)
- Duty of referees to protect participants.

Mazze v. Manhattanville Coll., 226 A.D.3rd 887 (N.Y. App. 2024)
- Soccer player injured while weight training.

Naimoli v. Pro-Football, Inc., 120 F.4th 380 (4th Cir. 2024)
- Limiting negligence liability through purchased ticket terms.

Turner v. NFL, 307 F.R.D. 351 (2015)
- Failure to protect NFL players from known danger of concussions in professional football.

Walton v. Premier Soccer Club, Inc., 2025 Md. LEXIS 143 (Md. 2025)
- Failure to follow concussion safety legislation.

TEACH LIKE A PARK RANGER: USING PARK INTERPRETATION TECHNIQUES TO TEACH BUSINESS LAW

MATTHEW D. MANGUM*

ABSTRACT

Park rangers use a method called interpretation to facilitate meaningful experiences for park visitors. Interpretation is not instruction, but an approach that inspires visitors to connect to a park site and have a memorable experience. College students can benefit from this intentional approach to developing personal connections and business law instructors can use lessons from park interpretation to do just that. This paper will set out the basics of park interpretation as used by the National Park Service and provide examples of how it can be used in the college classroom.

I. INTRODUCTION

When teaching the Implied Warranty of Merchantability, it is common to use *Webster v. Blue Ship Tea Room*[1]. The case revolves around a bone in a bowl of fish chowder. As I teach in south Texas, fish chowder is not a common experience for my students, so I modify the example to be about *enchiladas verdes de pollo*—green chicken enchiladas—a far more common experience for the students in my courses. By doing this, the students' past experiences help them relate to the legal rule from the case and make it more approachable because it is connected to their own lives. Even better than providing the class with an analogous situation is to have the students come with their own examples where the same rule would apply. This technique is the same approach used by park rangers. Perhaps you have visited one of the more than 400 national parks scattered across the country and found that you had a meaningful experience. Well, that is no accident. The National Park Service (NPS) intentionally designs their wayside signs, brochures, and ranger led programs to facilitate that happening. For example, at Mission San Juan Capistrano, part of San Antonio Missions National Historical Park, the hand-dug irrigation system—called an acequia—is still in use. A visitor to the park might look at these and see nothing more than a ditch. However, if a ranger points out that the acequias are still irrigating fields that are cultivated by the San Antonio Food Bank so that the site still feeds the community as it has since 1731, a connection can be made.[2] The acequia is not some old ditch, but it is a functioning, living tool for survival

* M.A., J.D., LL.M., Clinical Associate Professor, Texas A&M University-San Antonio & Volunteer-in-Park, San Antonio Missions National Historical Park

** Special thanks to Dr. Amy Lewis and National Park Rangers PT Lathrop, Maggie Burkett, Ariana Quazi, Andrew Shirey, William Bozic, and Chantelle Ruidant-Hansen for your encouragement, sharing resources, and providing feedback. Also, with gratitude to all the past and present Rangers and Volunteers of San Antonio Missions National Historical Park. I am grateful for all that I have learned from you.

[1] 347 Mass. 421, 198 N.E.2d 309 (1964)

[2] *Mission San Juan*, NATIONAL PARK SERVICE, https://www.nps.gov/saan/planyourvisit/sanjuan.htm (last visited Mar. 12, 2025).

that people universally can understand as needed to sustain life. Business Law instructors can do the same thing by utilizing the techniques of park interpretation in their classrooms.

II. WHAT IS INTERPRETATION?

Freeman Tilden, a seminal figure in the development of the National Park Service's understanding of interpretation writing in the 1950s, defined it as "An educational activity which aims to reveal meanings and relationships through the use of original objects, by firsthand experience, and by illustrative media, rather than simply to communicate factual information."[3] Interpretation[4] is a mindset and technique used by park rangers to connect visitors to natural, historic, and cultural sites they are visiting. Interpretation is not bombarding someone with facts. Instead, it is about fostering a personal connection between a visitor and the resource visited. This historic artifact is connected to a universal theme everyone can connect to. This process matches well with the purpose of a college education which is more than simply learning facts. When teaching Business Law, it is easy to bombard students with statutes, cases, and regulations. However, the educational experience can be made more meaningful if the students can connect to the rules in a meaningful way such as when a case revolving around a traditional dish served in a different part of the country is connected to a traditional dish from the students' home.

A. Classical Interpretation[5]

After thorough observations of NPS practices, Tilden drafted six principles of interpretation. They are:

> 1. Any interpretation that does not somehow relate what is being displayed or described to something within the personality or experience of the visitor will be sterile.
> 2. Information, as such, is not interpretation. Interpretation is revelation based upon information. But they are entirely different things. However, all interpretation includes information.
> 3. Interpretation is an art, which combines many arts, whether the materials presented are scientific, historical or architectural. Any art is in some degree teachable.
> 4. The chief aim of Interpretation is not instruction, but provocation.
> 5. Interpretation should aim to present a whole rather than a part and must address itself to the whole man rather than any phase.
> 6. Interpretation addressed to children (say, up to the age of twelve) should not be a dilution of the presentation to adults but should follow a fundamentally different approach. To be at its best, it will require a separate program.[6]

---

[3] FREEMAN TILDEN, INTERPRETING OUR HERITAGE 33 (2007).
[4] John Muir, a noted naturalist, is credited as first using the term in this context. *See* NATIONAL PARK SERVICE, FOUNDATIONAL OF INTERPRETATION CURRICULUM CONTENT NARRATIVE 2 (2007), https://www.nps.gov/idp/interp/101/foundationscurriculum.pdf
[5] Although this is not that designation used in the literature, it captures the importance and foundational nature of the early works on the subject.
[6] Tilden, *supra* at 18.

These principles remain the philosophical foundation of park interpretation. Most of these principles can be applied to higher education. Tilden himself draws a connection between his first principle and college education. "The reason why our college graduates, in past decades, have spoken with such reverence and affection of certain teachers…was because such men by universality of mind instinctively went behind the body of information to project the soul of things."[7] Professors—and park rangers—who are passionate about the object of their teaching want to share that with learners. Passionate professors know it is important to convey the essence of the field. When teaching, our goal should not be to teach students an assortment of vaguely connected aspects of the discipline, but an understanding of what it really is, its purpose, and how it impacts society. Teaching business law should not be a hodgepodge of statutes and rulings. Instead, business law professors should strive to communicate the goals and reasoning of law. Further, the subject needs to connect to the students and their lives. Law should not be presented in a vacuum, but in the context of how it impacts lives.

The second principle is an important reminder not to bombard learners with too many facts. Perhaps you have been on a tour and the guide shared fact after fact about everything you saw. How much of that did you remember when the tour was over? A park ranger is likely to focus on a few important facts that will help visitors see connections which they are more likely to remember. Tilden writes "…it is far better that the visitor to a preserved area, natural, historic, or prehistoric, should leave with one or more whole pictures in his mind than with a mélange of information that leaves him in doubt as to the essence of the place, and even in doubt as to why the area has been preserved at all."[8] For example, if you visit Redwood National and State Parks, you could be overwhelmed by minutia about the trees, other plants, the coast, animals, climate, and many other things. Instead of giving a long lecture about all those things, a ranger might focus on the relationship between the very large redwoods and the (comparatively) very small banana slugs.[9] Learning about their fundamental interconnectedness is something you are more likely to remember in the long term. In the same way, it is easy to overwhelm students with details of the Uniform Commercial Code (UCC), however well-crafted examples such as a modified *Blue Ship Tea Room* make important aspects more memorable.

In his fourth principle, Tilden makes it clear that park visitors should be changed by the experience. "But the purpose of interpretation is to stimulate the reader or hearer toward a desire to widen his horizon of interests and knowledge, and to gain an understanding of the greater truths that lie behind any statements of fact."[10] Interpretation, however, does not end there; it also seeks to provoke. Often the goal is to guide visitors to see why a resource is worth protecting. For example, reading the wayside signs, watching the park film, or going on a ranger led hike in the redwoods, might help them see why the ecosystem is so special. The visitor might begin to think that those plants and animals are worth protecting. That experience may lead them to support the preservation of that ecosystem and others like it. If students have a meaningful experience learning about law, they may have more respect for the rule of law or perhaps even wish to engage in making the law better.

---

[7] *Id* at 27.
[8] *Id* at 69.
[9] *Banana Slug & Millipede*, NATIONAL PARK SERVICE, https://www.nps.gov/redw/learn/nature/banana-slug-and-millipede.htm (last visited Mar. 12, 2025).
[10] Tilden, *supra* at 59.

In part, principle 5 combines principles 1, 2, and 4. Providing the right amount of information and trying to provoke a response (in a positive way), while making the material relevant to the visitor or student means that they will have the most valuable experience possible. When this goes well, visitors and students will not only learn about specific aspects of a resource or the law but will understand what they have seen in context. The right presentation of rules and case problems will help students appreciate law, the legal system, and legal reasoning.

B. Turn of the Century Interpretation/Meaning Interpretation

While Tilden sets out the theoretical foundation, park interpreters in the late twentieth and early twenty-first centuries turned their focus to techniques to achieve interpretation's lofty goals. They begin with a simplified set of three tenets. First, "Resources possess meanings and have relevance."[11] Second, "Audiences seek something of value for themselves."[12] Third, "Interpretation facilitates a connection between the meanings of the resource and the interests of the visitor."[13] Certainly law is relevant in the professional lives of those studying business. It is also true that students seek knowledge of law that will help them in their lives and careers. Central to the turn of the century approach to build connections is the importance of a good theme.

Clearly framing the material presented was seen as essential to helping visitors have a meaningful experience. A good interpretive theme combines two things: a tangible object and an intangible meaning. Visitors come to parks to see tangible objects—mountains, tress, bison, 300-year-old missions, battlefields, and many other physical resources. Business law students come to class to learn about statutes, regulations, and cases. Park rangers help visitors connect to those objects by connecting them to universal concepts which are approachable by many people. "The most compelling and broadly relevant meanings are universal concepts, ideas and notions that almost everyone can relate to, but do not mean the same to any two people. Examples of universal concepts include: joy, death, family, suffering, love, and birth."[14] Business law could be connected to such universals as justice, fairness, due process, or cooperation.

In addition to serving as a kind of thesis for a presentation, a theme is also the takeaway the visitor or student should remember. "At the completion of any interpretive presentation, the audience should be able to tell you what was said by summarizing it in one sentence. This sentence is the theme, the central or key idea of any presentation."[15] This means that the entire presentation should be framed and structured to convey and support the theme. An example would be, "The amazing and strange saguaro is both a barometer of the health of the desert and a fragile victim of human errors."[16] This combines the tangible cactus with the themes of health and fragility. Similarly, discussions of UCC implied warranties can combine cases with concepts such as safety and legal liability.

Turn of the century's approach is incapsulated in the Interpretive Equation. (Knowledge of the Resource + Knowledge of the Audience) x Appropriate Techniques = Interpretive Opportunity.[17] This means that the ranger must know their resource well. They must also know

---

[11] DAVID L. LARSEN, MEANINGFUL INTERPRETATION 12 (2011).
[12] *Id* at 22.
[13] *Id* at 37.
[14] *Id* at 91.
[15] WILLIAM J. LEWIS, INTERPRETING FOR PARK VISITORS 37-38 (1991).
[16] Larsen, *supra* at 25.
[17] *Id* at 216.

their audience and what universals will relate to them and be able to adapt programming based on who is listing. Then can then be communicated through various techniques. The business law professor must know the law, must know their students, and must use the teaching techniques that work in the context of their class.

Just as Tilden stated that the goal of interpretation was to provoke, turn of the century interpretation also wants visitors to experience a change. "Interpretation strives to establish a relationship of care."[18] A major ask of interpretation is helping visitors think about why they should care about the subject. Learning about acequias, redwoods, slugs, and other resources helps the visitor care about those places, plants, and animals. In the same way, learning about statutes and cases can help a student care about law.

C. Twenty-First Century Interpretation/Audience Centered Interpretation

Since the 2010s, the NPS has worked on updating its interpretative model. The twenty-first century version of interpretation is investigative, participatory, collaborative, and skills-focused.[19] Among the skills are critical thinking and communication.[20] At its core, this version of interpretation aims at making the visitor the heart of the process. Hence it is also known as Audience Centered Interpretation or ACE. A similar evolution has been seen in higher education as both about moved away from an exclusively sage-on-the-stage model of education.[21]

A key aspect of twenty-first century interpretation is putting the visitor at the center of the experience while still being resource driven. "The resource is the battery that powers the visitors as they shine."[22] Rangers focus on audience engagement and trust the visitor's curiosity. "The audience is given an opportunity to answer questions about their own lives. The interpreter reacts to those answers, offering content about the resource…"[23] By responding to visitors' answers with factual information and stories about the tangible resource, it is the audience that guides the experience of the park. To do this, rangers use essential theme questions. "An essential theme question connects your site's stories to personally relevant and socially significant issues, and guides the focus of the visitor experience."[24] These questions should be intriguing, complex, based on problems facing society and for critical thinking and thoughtful discussion. An example relevant to teaching law would be, "Who has the right to define 'justice?'"[25] Such a question could lead to a discussion of why laws are created, how they are interpreted, and the role people play in the process. These questions allow for learners to make meaningful connections because their experiences are front and center. They also allow visitors to come to conclusions about what they are seeing on their own, rather than being told what to think.

Twenty-first century interpretation also updates the Interpretive formula. (Knowledge of the Audience + Knowledge of the Resource + Knowledge of Self) x Appropriate Techniques = Interpretive Opportunity.[26] While knowledge of the resource and of the audience are very

---

[18] *Id* at 49.
[19] NATIONAL PARK SERVICE, FORGING CONNECTIONS THROUGH AUDIENCE CENTERED EXPERIENCES 2 (2018).
[20] NATIONAL PARK SERVICE, FORGING CONNECTIONS THROUGH AUDIENCE-CENTERED EXPERIENCES: TRAIN THE TRAINER 3 (2023).
[21] NATIONAL PARK SERVICE, FORGING CONNECTIONS THROUGH AUDIENCE CENTERED EXPERIENCES 4 (2017).
[22] TRAIN THE TRAINER, *supra* at 4.
[23] *Id*.
[24] FORGING CONNECTIONS THROUGH AUDIENCE CENTERED EXPERIENCES (2018), *supra* at 8.
[25] *Id*.
[26] TRAIN THE TRAINER, *supra* at 18.

important, it adds knowledge of self. This is a kind of emotional intelligence that requires awareness of conscious and unconscious bias and expressing one's thoughts and feelings in a professional manner.[27]

An audience-centered experience has four parts. First, it tells a great story and invites visitors to share stories too. Second, invites sharing through asking and answering questions that get to the universal human experience. Third, it allows learning from & with others. Finally, it grapples with a sticky problem and helps visitors see things in a new light.[28] This model is more interactive than classical interpretation. Having students think of similar examples to *Blue Ship Tea Room* based on foods they know and have eaten makes learning business law more student centered.

Audience-centered interpretation uses the MuseumHack Ethic of using a traffic light scale of green, yellow, and red-light experiences.[29] Rangers can build rapport with visitors with safe or green questions and experience. At this stage a ranger might ask where visitors are from and invite them to walk around a space or take photographs. Rangers can then move to intermediate or yellow actives that ask visitors to answer more complex questions that may require the visitor to share about their personal experiences. Finally, the ranger may try for more risky or red questions which ask visitors to engage in a more personal way. These questions might have visitors engage in critical thinking about an important issue connected with the resource. Over the course of a class or semester, business law professors could build from green to red light experiences. They may begin on the first day by asking about students majors or interests and move to more critical and personal reflections about important issues by the end of the term.

III. APPLICATION TO TEACHING BUSINESS LAW

When applying interpretation techniques to teaching business law, the first step is to identify if there is a resource or object of interpretation. The law and the American legal system can be viewed as part of our shared cultural heritage, with constitutions, statutes, regulations, and court opinions serving as the tangible objects of that heritage. Business law professors can help students encounter specific rules and rulings and have a meaningful experience that helps them understand and appreciate the legal system and the rule of law. Further, with the stated goals of increasing critical thinking and improving communication skills, twenty-first century interpretation shares learning outcomes with higher education.[30] In fact, those are two of the college wide, programmatic learning outcomes at my own college. With shared goals, there are several lessons college faculty can learn from park rangers.

A. Know your Audience

It's important to know who your students are. Professors can do this on many different levels. Knowing the demographics of one's college or university will give some insight into who will be in our classrooms. Further, faculty should consider individual sections of a course. For examples, day classes may have more younger students while evening classes may have more working adults. These different groups will bring their own experiences and likely connect to

[27] FORGING CONNECTIONS THROUGH AUDIENCE CENTERED EXPERIENCES (2018), *supra* at 19.
[28] TRAIN THE TRAINER, *supra* at 19.
[29] FORGING CONNECTIONS THROUGH AUDIENCE CENTERED EXPERIENCES (2018), *supra* at 14.
[30] TRAIN THE TRAINER, *supra* at 3.

different examples and material. For example, pop culture references that work with one class may not work in another. One of the most useful things to do is to inquire as to why are the students are there and what do they expect and want to learn. Students take classes for many different reasons. Some will be there simply because it is a requirement for their major. Others will be there because of want to learn information that is relevant to their own small businesses. Others may aspire to graduate school or law school. Knowing these motivations can help a professor tailor the course and examples in a way that fosters making meaningful connections.

B. Use a Clear Theme

Interpretive themes are the thesis of a program. They connect the resource to a universal and provide a focus. These can easily be used for a class lecture or discussion. I usually begin the discussion of contracts with this theme: Contracts are legally enforceable promises. The resource in question is the body of contract law made up the restatement, statutes, and court opinions and specific contracts themselves. The universal is a promise. Students, like most people in the world, will understand what a promise is. Everything presented in class while discussing contract should help students see and remember make makes a contract a promise that a court of law will enforce. With that basis, students are more likely to engage and remember important aspects such of the elements that make a promise legally enforceable.

C. Use Students' Experiences as a Starting Point

Whenever possible, ground the discussion of legal concepts in student experiences. One way to do this is using student generated examples. For example, ask students what contracts they are a party to. Perhaps they will offer their apartment lease, cell phone agreement, or a streaming service's terms and conditions. These can then be used to discuss the elements of a contract and other important topics. Because these are examples from their experience, students are more likely to connect to them. Contracts are not some nebulous thing businesspeople use; they are agreements that students have already entered. Further, if a student in the class has a small business making and selling goods—e.g. stickers or air fresheners—use that as an example of a good when discussing the UCC. Instead of a randomly selected widget, students can connect because it is a product their classmate sells.

D. Don't Go Overboard with Information

Perhaps the most important lesson is not to overwhelm students with information, but to inspire students' interest in and connection to the law. As lawyers know, the law is vast and complex. There can be a temptation to teach students as much of the law as possible in a term. However, doing so may cause students to miss the big picture. Instead of memorizing lots of statutes and precedent, it is more important that students understand certain key principles and how the law reasons. By focusing on a smaller number of essential topics, students can engage with them and have a better opportunity to explore how they work and how they apply to their own lives or business dealings. Professors can reflect on the things they must want students to remember—perhaps the elements of a contract or legal reasoning—and help students connect to those themes.

E. Make Connections to Other Classes

The stories of national parks often overlap.[31] San Antonio Missions National Historical Park tells the story of Spanish colonialism, Palo Alto Battlefield National Historical Park tells the story of the Mexican-American War, and Chamizal National Memorial tells the story of the United States and Mexico reaching a treaty to recognize a definite border. Together, these parks tell a connected story that spans 1718 until 1963 and beyond. When these stories are connected, visitors can better understand the history of Texas, Mexico, and the United States. When teaching business law, professors must make the same kind of connections. Law intersects with the accounting, management, marketing, and ethics classes that the students are taking. When relevant it is important to point out those connections to students. Knowing the majors of students in the class and nudging them to make the connections is a possible approach. Helping students see the interconnectedness is an important aspect of the course. Business law professors might expressly ask students to think of examples from their other courses that are relevant to the topic being covered.

F. Solve Problems & Work Together

Law is highly driven by cases. Although a standard technique of teaching law, having students work together to solve case problems in an excellent way to have them engage with law and make connections. This allows students to practice critical thinking skills and grapple with legal questions. When working through problems themselves, they are more likely to form a connection to the material. This engagement puts the student and the center of the experience.

G. Create a Brave Space for Questions

It is important that classrooms are safe spaces for students to ask questions. That means having a welcoming environment, building rapport, and encouraging listening. Asking questions that are inviting, non-judgmental, and generative can help create such a place.[32] However, a safe space is not enough. The NPS uses the idea of a brave space. This space allows for conversation with a diversity of views while recognizing that learning is messy and needs guidance. To get to this point, instructors must build rapport and trust with students. In every class, an instructor is likely to ask green light questions that get to basic definitions and rules found in the textbook. Students will also be asked yellow light questions such as to solve a case problem and explain their answer. Because it involves their own reasoning and the possibility of being incorrect, it requires the right classroom conditions to exist. On occasion, class discussion may involve more red light questions such as discussions of complex and important topics in a way that provokes students to think about other perspectives and engage in critical reflection. An example of such an endeavor would be discussing the rule of law and how well our legal system achieves those goals. This might be best approached at the end of term after the professor and students have worked together for weeks and built a classroom community where students know they are able to engage.

---

[31] NATIONAL PARK SERVICE, VISION PAPER: 21ST CENTURY NATIONAL PARK SERVICE INTERPRETIVE SKILLS 8 (2014).
[32] TRAIN THE TRAINER, *supra* at 13.

H. Follow Student Curiosity

Students will often have questions about law. These may have their origin in current events, the student's own life, or other classes the student is enrolled in. Although not always fully on topic, these can be an excellent opportunity to teach fundamentals of law. When possible, the professor can connect the question to topics covered in the course. The benefits of a short tangent can increase student engagement can help connect the issues they are curious about to the topics of the course. For example, nearly every semester, a student will ask about the legal status of cannabis. Although this is not a topic of the course, answering the question involves discussion of the difference between federal and state law, prosecutorial discretion, banking regulations, and the legal risks of some businesses. So, taking the time to answer the question connects to many important concepts in the course. Fielding these kinds of questions lets the students know they are an important part of the learning process.

I. Stay Up to Date

Knowledge of the resource is an essential for interpretation. However, the understanding of resources changes over time. Historical, archeological, and biological research is ongoing and new things are learned. Because of this, rangers are instructed to stay up to date with the latest research on their parks.[33] In much the same way, law is constantly changing. For business law professors, it's important to stay on top of the latest legal trends and to learn new and current examples to use in class. Thoughtfully engaging continuing legal education is important to this goal. Further, professional development on teaching techniques and pedagogy can also help professors remain effective teachers.

J. Tell a Good Story

Park rangers are famous for being good story tellers. Luckily for business law professors, often cases are good stories. Telling those stories can help students connect to seemingly abstract legal rules. For example, when discussing equal protection, telling the story of the Little Rock Nine integrating Little Rock Central High School—now a National Historic Site—brings the rule to life.[34] In *Blue Ship Tea Room*, the court tells a story to explain why the plaintiff should have known that fish bones were likely in traditional fish chowder. When teaching contract law, cases such as *Leonard v. PepsiCo*[35] and *Vokes v. Arthur Murray*[36] are examples of interesting fact patterns that can be used to help students learn legal principles through stories.

IV. CONCLUSION

In the end, it is important to note that park interpretation and college teaching are not identical activities. Professors must require students to remember some important facts, like the elements of a contract. Professors must assess if the students have mastered the material though

[33] NATIONAL PARK SERVICE, INTERPRETATION AND EDUCATION 7.5.4.
[34] *History + Culture*, NATIONAL PARK SERVICE, https://www.nps.gov/chsc/learn/history-culture.htm (last visited Mar. 12, 2025).
[35] 88 F. SUPP. 2D 116 (S.D.N.Y. 1999).
[36] 212 SO.2D 906 (FLA. 2D DCA 1968).

homework, exams, and papers. Professors must assign grades to students. However, the tools of park interpretation have much to offer the college professor. Making the effort to know who your students are, to tailor your examples and get students involved in creating there their own, focusing on the important aspects of law without losing the forest for the trees, and using a clear theme to tell a good story will facilitate a meaning learning experience for the students. When it goes right, students will be more involved and more likely to remember fundamental legal principles after the course ends.

DRUG LEGALIZATION AND EMPLOYER LIABILITY: HUMAN RESOURCES PROFESSIONALS WHO REDUCE THE RISK OF CIVIL LITIGATION MAY ALSO REDUCE THE RISK OF CRIMINAL PROSECUTION

RICHARD O. PARRY*

I. INTRODUCTION

When it comes to employment-related litigation, human resource professionals are a business organization's first line of defense. Arguably, the greatest threat of litigation to a business are lawsuits by employees and former employees, usually alleging wrongful termination, harassment or discrimination. Educating both its workforce, as well as its human resources professionals can do much to reduce the threat of this litigation (although there is nothing that can be done to eliminate this threat).

However, there are other issues that, although less likely, are just as much a threat to a business organization and again, it is education and human resource professionals that are a business organization's first line of defense. Business organizations face an alphabet soup of regulations that demand compliance. Whether it is antitrust (including, but not limited to the Sherman Antitrust Act, the Clayton Act and the Robinson-Patman Act among others), environmental protection (including, but not limited to the Clean Air Act, the Federal Water Pollution Control Act, the Safe Drinking Water Act, among numerous others), or the tax laws, organizations face a complex web of laws that are demanding and unforgiving of noncompliance or misinterpretation.

In addition, the potential for criminal prosecution of a business as well as its officers, directors and employees should not be underestimated. The Racketeer Influenced Corrupt Organizations (hereinafter "RICO") Act (18 U.S.C. §§ 1961-1968), enacted in 1970, and intended to address organized crime, also allows for civil litigation of some matters. Because Congress mandated that RICO "be liberally construed to effectuate its remedial purposes"[1] the United States Supreme Court has held that RICO may be applied to legitimate businesses,[2] allowing private plaintiffs and the government to file civil actions.[3] The reasoning behind this is simple.

The government lacks the resources to prosecute every RICO violation. This allows, perhaps even invites, creative attorneys to apply its harsh penalties and, especially, its generous financial rewards, to cases that have no apparent connection to what is traditionally considered criminal activity, but that arguably constitutes unethical behavior.

* J.D. Professor. California State University, Fullerton.

[1] Pub.L. No. 91-452, § 904(a), 84 Stat. 942 (1970); see also United States v. Turkette, 452 U.S. 576, 587 (1981).

[2] See, for instance, Sedima, S.P.R.L. v. Imrex Co., 473 U.S. 479, 499 (1985)

[3] 18 U.S.C. § 1964(b).

For instance, bribery may give rise to both criminal prosecution as well as civil lawsuits against an employer that tolerates, or sometimes encourages, it,[4] as well as those that paid the bribes and even the law firms and individual attorneys at the law firms that knew of the bribery. RICO provides for exceptionally generous financial rewards for a successful plaintiff, such as treble damages and attorneys' fees.

While the threat of criminal prosecution of business organizations because of a violation of these laws is likely to be low, because of illegal activity and unethical behavior by a very small number of large companies, business organizations now face an environment where there is little tolerance by the government, or juries, for illegal or unethical behavior.

What may have been treated as negligence, and something to be remedied by civil litigation in the past is now the subject of criminal prosecution. While this approach has been criticized,[5] the government's intolerance has been shaped by some notable cases.[6] With the foregoing in mind, this is a review of the threats that human resource professionals traditionally face, along with other threats that, while less likely, have the potential to be even more devastating to a business organization.

II. EMPLOYMENT-AT-WILL

Normally, either the employer or employee can terminate the employment relationship at any time and for any reason unless a contract provides to the contrary.[7] In California, and many other states as well, employment is presumed to be an at-will relationship as long as there is no other method of termination to which the parties have agreed in a contract and as long as the employment is not for a fixed length of time.

Although courts tend to trumpet employment-at-will as the "law of the land,"[8] as numerous commentators have noted, there are exceptions. For instance, does an employee feel that the employment relationship will not end unless there is a good reason (sometimes called "good cause[9]")? It is not unusual for an employee to develop a belief (and an employer may encourage

---

[4] See, among numerous other lawsuits, In re American Honda Motor Co., Inc. Dealership Relations Litigation, 979 F. Supp. 365 (1997).

[5] See, for instance, Trapped: When Acting Ethically is Against the Law (2006) by Professor John Hasnas.

[6] See, for instance, In re American Honda Motor Co., Inc. Dealerships Relations Litigation, 958 F. Supp. 1045 (1997).

[7] In 1895, Montana enacted a statute that recognized employment-at-will. This statute was repealed in 2001. However, prior to that, in 1987, Montana became the only state to enact a statute that required a "good cause" standard for the discharge of at-will employees. This statute did not represent a complete victory for at-will employees. Among other restrictions, the statute limited recovery to four years of lost wages and fringe benefits and eliminated damages for pain, suffering and emotional distress. The law also made it more difficult to recover punitive damages and limited the recovery of punitive damages to actions based on a violation of public policy. The restrictions led one commentator to observe, "…the apparently increased protection afforded workers by the WDFEA's establishment of a 'good cause' requirement for terminating employees was deceptive. In reality, the heightened standard, combined with the additional procedural and substantive hurdles, provided less protection against discharge than 'good cause' typically implies, and it may even have provided less protection than the common law it replaced." See Ewing, North and Taylor, "The Employment Effects of a 'Good Cause" Discharge Standard in Montana." Cornell University Industrial & Labor Relations Review, October, 2005 (59 Ind. & Lab. Rel. Rev. 17, 21).

[8] See, for instance, California Labor Code Section 2922, affirming employment-at-will as the " law of the land" (unless otherwise agreed or an exception exists) as well as *Foley v. Interactive Data Corp*., 47 Cal. 3d 654 (1988).

[9] The Model Employment Termination Act (META) notes, in Section 3(a), "…an employer may not

such a belief), that an employee will not be discharged merely at the whim of the employer. Does the employee have a legitimate right to expect that his employer will not terminate employees arbitrarily?

If the employment relationship has changed into one in which both the employer and the employee (or employees) agree that there will be no discharge without good cause, employment-at-will doctrine may no longer control. The change is unimportant until there is a dispute over the existence of "good cause" for a termination.

In a classic catch-22, an employer that approaches discipline and termination issues with an interest in assuring that all such decisions are fairly reached is more likely to convince a court that it has abandoned employment-at-will. However, it has also been noted[10] that an employee's perception of the fairness of an employer's decision-making process is also likely to affect the likelihood that an employee will file a wrongful-termination lawsuit.

A. *Exceptions to the Employment-at-Will Doctrine*

1. Exceptions Based on Contract Theory

A relatively few number of employees have express contracts of employment, usually for a definite duration. An express contract has terms spelled out by the parties, usually in writing. More employees are covered by collective bargaining agreements that are negotiated by a union. Most workers have no express agreement as to the term of their employment, although some may have been given an oral promise of a fixed term of employment in a jurisdiction in which the statute of frauds requires that contracts for performance beyond a year or more be written.

Some of those employees have then tried to convince a court that there exists an implied promise. Implied contracts are those that courts infer from company policies, for instance, in an employee handbook, the behavior of the parties, or implied by law.

A company's personnel handbook that says, for example, that employees will be fired only for certain specified violations of work rules, or that the firm will follow a specified procedure when disciplining an employee, may give rise to a terminated employee's argument to a court that the handbook became a part of the terminated employee's contract with the company. An increasing number of courts accept this argument. This is reinforced when employees are led to believe that they can reasonably rely on these policies, for instance in statements by upper management.

A few courts go even further and find an implied covenant of good faith and fair dealing. This seems to be a court-ordered requirement that an involuntary termination be for just cause. The standard for "just cause" is determined on a case-by-case basis. This requires an employer to deal fairly and in good faith with all employees, even an at-will employee.

---

terminate the employment of an employee without good cause." However, Section 3(b) limits application of "good cause" to workers who have been with the particular employer for at least one year. Section 4(c) adds another exception, allowing an employer and employee to substitute a severance pay agreement for the good cause standard. Section 4(c) also notes that the good cause standard is inapplicable to situations where termination comes at the expiration of an express oral or written contract containing a fixed duration for the employment relationship. Because of deep divisions the META has not achieved uniformity and states have been encouraged to modify the model to suit their particular needs.

[10] Gillespie and Parry, Fuel for Litigation? Links Between Procedural Justice and Multisource Feedback, Journal of Managerial Issues, Winter, 2006, Volume 18, No. 4.

Employment, whether express or implied or for a fixed or an undetermined term, may be considered a contractual relationship.[11] A wrongful termination claim based on breach of contract claims that an employer made an enforceable promise and then breached that promise.

All documentation, including, but not limited to employee handbooks, may be used by a court to determine the terms and conditions of an employment contract.

2. Oral Promises

A terminated employee may contend that the employer modified or waived the established "at-will" relationship, as a result of representations, for example, resulting in an implied-in-fact promise that the employer would not discharge employees except for "good cause."

It is usually the employer's conduct that gives rise to a claim that the employment-at-will doctrine has been modified or abandoned. For instance, many employers set up a system to ensure that adverse employment actions are fair:

1. The employer may require an investigation of the issue, with a report submitted to a decision-maker;
2. There may be a hierarchy of decision-making that is dependent on the length of service of the employee or the rank of the employee;
3. There may be a progressive discipline system;

Regardless, the implication is that the employer's decisions are not "arbitrary and capricious" while being careful and concerned, with an emphasis on fairness and acting responsibly for a good reason.

All of these policies imply that the relationship is not "at will" but rather requires "good cause." Thus, it is reasonably easy for a plaintiff to establish an implied-in-fact "for-cause" employment relationship which means that it is likely the plaintiff's case will be heard by a jury. Juries decide questions of fact, whereas the judge will decide questions of law. Whether there is sufficient cause to terminate is likely to be a question of fact for a jury. Because of the expense of defending a lawsuit through trial and possible appeal, as well as the uncertainty that goes with a jury's decision, this increases the settlement value of such a lawsuit.

The significant question for the jury is: Was the decision to terminate proper or not? Since there is rarely direct evidence on the issue of decision-making, circumstantial evidence with all the attendant speculation that goes along with it, may be critical.[12]

3. Exceptions Based on Law

While the employment relationship is fundamentally contractual, federal and state laws have imposed a number of restrictions on the actions of employers. The Sarbanes-Oxley Act includes two provisions, one criminal and the other civil, for the protection of employees who

[11] See, for example, California Labor Code Section 2750

[12] In *Coltran v. Rollins Hudig Hall International, Inc.* 17 Cal.4th 93 (1998) the California Supreme Court held that "The proper inquiry for the jury….is not, 'Did the employee in fact commit the act leading to dismissal?' it is, 'Was the factual basis upon which the employer concluded a dischargeable act had been committed reached honestly, after appropriate investigation and for reasons that are not arbitrary or pretextual."

report improper conduct by corporate officials related to securities fraud and corruption. Other legislation, ranging from the National Labor Relations Act (29 U.S.C. § 158(a)(1),(3),(4) [precluding discharge for union activity, protected concerted activity, filing charges and testifying under the act]) to title VII of the Civil Rights Act of 1964 (42 U.S.C. §§ 2000e-2, 2000e-3(a) [prohibiting discharge on the basis of race, color, religion, sex or national origin or for exercising rights under the act]), and state statutes precluding discharge for filing workers' compensation claims or in violation of state civil rights statutes, significantly circumscribe the at-will doctrine.

Generally, employment decisions cannot be based on race, gender, religion, color, national origin, age, disability, marital status, pregnancy or medical condition. Some state and local governments may include additional forbidden grounds for termination. It is also a violation of the law to harass any employee in his or her employment because of these grounds, or to retaliate against an employee because he alleged wrongdoing, or assisted in the defense or prosecution of an alleged adverse employment action based on one of these prohibited grounds. All at-will employees are protected against decisions based on any of these specified bases.

In this situation, protection against discrimination is based on law and has nothing to do with the employment contract. Thus, if a former employee can show that the termination was wrongful because it breached a law, the actions of the employer are in violation of the law and now the employee is not limited to contractual remedies. This is likely to mean that the potential verdict against the employer will be much larger, and may include significant negative publicity.[13]

Most lawsuits that allege discrimination are "disparate treatment" (which are to be distinguished from "disparate impact") cases. In a disparate treatment case, the employee claims that he or she suffered an adverse employment action because he or she was treated differently than other similarly situated employees and the treatment was based on a prohibited ground. "Disparate impact" refers to a situation where, for example, an employer's policies had a disparate impact on an employee.[14]

However, even in those rare situations where no federal or state protection against retaliation exists, a court is likely to find a public policy exception to employment-at-will if a terminated employee is able to show that he was fired for attempting to report or correct illegal company activity, for example.

4. Exceptions Based on Public Policy

This is the most likely exception to the employment-at-will doctrine. This exception arises when the discharge is contrary to an important public policy. While this is not easily defined, it generally means that an employee may not be fired for exercising a legal right or fulfilling a legal duty.[15]

---

[13] The only restriction on the employee is the requirement that they exhaust the administrative remedies that are specified in the law before filing a lawsuit. This is unlikely to prove a significant factor for the employer.

[14] See, for example, *Griggs v. Duke Power Co*., 401 U.S. 424 (1971), where an employer's policy of requiring a high school diploma was shown to have a "disparate impact" on African Americans.

[15] For example, most states hold that an employer cannot fire an employee who misses work for jury duty, as long as the employee has given the employer the appropriate notice. However, this exception is far broader than that.

One court announced a four-step process to determine if there has been a violation of public policy:

1. Does a clear public policy exist?
2. Will that policy be jeopardized unless the activity in issue is protected;
3. Whether employers in general have overriding justification for wanting to use the activity in issue as a factor affecting the decision to discharge;
4. Whether the particular employee's activity in the case at bar was a substantial factor in (i.e. a cause of) the particular employer's decision to discharge.[16]

An employer may not discharge an at-will employee for, among other offenses: failing to comply with requests for sexual favors;[17] failing to comply with a request for perjurious testimony;[18] or failing to participate in a prohibited price-fixing scheme[19]

Although many courts recognize this exception to employment-at-will, courts also tend to also hold that the right or duty must be clearly spelled out by statute,[20] and the examples above are. However, this list is far from complete. Thus, if an employer terminates an employee in violation of a public policy, it means that the reason for the termination was "wrong," which, again, takes the termination outside the contract issue. Since the lawsuit is not based on contract, it gives rise to a tort cause of action.

[16] *Lins v. Children's Discovery Centers of America, Inc*. 95 Wash.App. 486 (1999)
[17] See, for example, *Jin v. Metropolitan Life insurance Co*., 295 F.3d 335 (2002) as well as *Rojo v. Kliger*, 52 Cal.3d 65 [1990].
[18] *Peterman v. International Brotherhood of Teamsters*, 174 Cal.App.2d, 184 (1959)
[19] *Tameny v. Atlantic Richfield Co*. 27 Cal.3d 167 (1980).
[20] See, for instance, *Geary v. United States Steel Corporation* 456 Pa. 171 (1974). In that case, the Pennsylvania Supreme Court, in reviewing a matter that had been dismissed by the trial court observed, "Geary's duties involved the sale of tubular products to the oil and gas industry. His employment was at will. The dismissal is said to have stemmed from a disagreement concerning one of the company's new products, a tubular casing designed for use under high pressure. Geary alleges that he believed the product had not been adequately tested and constituted a serious danger to anyone who used it; that he voiced his misgivings to his superiors and was ordered to 'follow directions,' which he agreed to do; that he nevertheless continued to express his reservations, taking his case to a vice-president in charge of sale of the product; that as a result of his efforts the product was reevaluated and withdrawn from the market; that he at all times performed his duties to the best of his ability and always acted with the best interests of the company and the general public in mind; and that because of these events he was summarily discharged without notice." The court, in ruling against Geary went on to note that the plaintiff did not possess any expert qualifications and that his duties did not extend to making judgments in matter of public safety.

Because the termination is more than a simple breach of contract issue, it violates important social values. Therefore, the employer's action is now considered an intentional tort and may result in punitive damages against the employer. When an employee files a lawsuit he or she will probably claim a violation of every one of the three categories noted above, plus several others, including:

1. Intentional infliction of emotional distress;
2. Fraud;
3. Invasion of privacy;
4. Defamation;
5. Intentional Infliction of Emotional Distress.

B. Intentional Infliction of Emotional Distress

Intentional infliction of emotional distress generally involves an intentional act that is considered extreme and outrageous conduct causing severe emotional distress to another.[21]

While emotional injuries arising out of termination of employment ordinarily are within the employee's regular course and scope of employment, and are thus preempted by the exclusive remedy of workers' compensation, if the employee was discharged for reasons that violate a statute or public policy, the termination is not deemed to be considered part of the normal workers' compensation issue and the employee is free to bring an independent tort claim of intentional infliction of emotional distress, along with the claimed breach of public policy. In addition, if the plaintiff claims a violation of tort law, pain and suffering resulting from the alleged wrongful termination may be recovered.

Annoyance is a part of everyday life, and usually insufficient to support such a claim, although some courts have held that repeated annoyance (by, for example, stalking), coupled with a credible threat, may be sufficient to satisfy the law's requirements.[22] While courts are generally reluctant to accept such claims, particularly since evaluation and criticism are part of the work environment, this is likely to be just one of several claims made by a former employee. For example, although employees are expected to be hardened to criticism, a court is not likely to view sexual harassment the same way, and a suit for sexual harassment is likely to include a claim for emotional distress.

C. Fraud

It may not be unusual for an interviewer to downplay negative information that may dissuade a prospective employee, to make promises regarding the duration of employment as well as the likelihood of promotions and pay raises. However, misrepresentations and unfulfilled promises may give rise to a number of claims, including fraud, negligent misrepresentation and breach of contract.[23]

---

[21] See, for example, Ford v. Revlon, Inc. 734 P.2d 580 (1987), where a manager, among other offenses, placed an employee in a chokehold and fondled her at a company picnic. The employee's complaints to management went unanswered for months.

[22] However, this may also implicate the First Amendment. See, e.g., Texas v. Johnson, 491 U.S. 397 (1989).

[23] See, for instance, see *Belknap v. Hale*, 463 U.S. 491 (1983) where an employer hired employees to take over the jobs of striking employees, with a promise of "permanent" employment. When the strike ended, the employees that were promised permanent employment were terminated and the striking employees reinstated. The Supreme Court ruled that the terminated employees could sue for breach of contract.

In the employment context, generally, an allegation of fraud arises when an employee claims that there was no intention on the part of the employer to be bound by a promise to terminate only for good cause, although other possibilities exist.[24] This requires the following:

1. At the time he or she was hired material misrepresentations were made by authorized personnel of the employer that the employee would only be terminated for good cause or the like;
2. The employee reasonably relied upon these representations.

A misrepresentation that may provide a cause of action for fraud or misrepresentation is not limited to outright falsehoods. Silence may satisfy the requirements when an employer selectively omits certain material facts with an intention of creating a false impression, or failing to correct a prior misrepresentation when advised of its inaccuracy.[25]

D. Invasion of Privacy

All people, including employees, have a right to solitude and privacy. And, while there are generally four different kinds of invasion of privacy that may be alleged by a plaintiff, in the employment context, an employee's allegation of an invasion of privacy by the employer generally arises in cases involving:

1. A discharge based on alleged sexual harassment or a claim that the employer disclosed personal information about an employee;
2. Adverse action taken against an employee based on a drug test.

One court used a three factor test to determine whether there has been an invasion of privacy:

1. The defendant must have publicized some aspect of the plaintiff's life;
2. That information must not be a legitimate concern of the public; and
3. Disclosure must be offensive to a reasonable person.[26]

An allegation of invasion of privacy by an employee is also likely to include a claim of defamation.

---

[24] See, for instance, *Mkparu v. Ohio Heart Care, Inc*., 740 N.E. 2d 293 (1999). A specialized medical practice sought to recruit a renowned specialist. The specialist was assured that he would be allowed to become an equal partner within a short period of time, which was critical to his decision. When the promised opportunity failed to materialize, the specialist sued and the appellate court affirmed a lower court's ruling that the specialist had been fraudulently induced to accept the position. The appellate court further remanded the case for consideration of punitive damages in light of the egregious conduct by the other doctors.

[25] See, for instance, *Stewart v. Jackson & Nash*, 976 F.2d 86 (1992).

[26] *Bodah v. Lakeville Motor Express, Inc.*, 663 N.W.2d 550 (2003). The key issue in the case was whether faxing the names and Social Security numbers of employees to sixteen terminals scattered across the U.S. constituted "publication." The Minnesota Supreme Court ruled that "publicized" means that, "…the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge." Having found that the fax did not meet this requirement, the court held in favor of the defendant.

E. Defamation

Defamation is generally defined as the publication of an untrue statement about an individual that harms the reputation of the individual, exposing the recipient to "hatred, ridicule or contempt." Defamation may be either written (libel) or slander (spoken). Potential examples of defamation in the employment context are:

1. An employer knowingly making false statements to one or more employees while attempting to make an example of the terminated employee;
2. An employer intentionally making false statements to a prospective employer with the intention of harming the discharged employee.[27]

The courts tend to treat slander and libel differently, for obvious reasons. A defamatory statement that is spoken has a transitory quality, while the same written defamation has a permanence to it, although modern communications technology may tend to blur the difference between the two.

Because the issue of opinion may be critical in the area of defamation, a court may hold that an opinion is defamatory only if it implies a statement of fact.[28]

F. Employers' Defenses to Defamation: Qualified privilege

There are several defenses to defamation available. The first defense is that of truth. However, the burden is on the employer to prove that the defamatory statement is true. Another defense, that of "absolute privilege" is ordinarily unavailable in the employment context. While there is a "qualified" privilege available to the employer, which may provide a defense, many employers correctly choose to avoid the issue by, for example, refusing to provide a reference. The justification for this is simple. When a company is protected by a "qualified" privilege, the alleged defamation cannot result in liability for the company as long as the alleged defamation was made in "good faith." However, this also means that the determination whether a "qualified" privilege exists is generally determined in a court, by a jury, with the attendant expense.[29]

---

[27] In California this may also violate California Labor Code Sec. 1050 and make the employer liable for triple damages.

[28] See, for instance, *Sagan v. Apple Computer, Inc*. 874 F. Supp. 1072 (1994) where the late Carl Sagan objected to the code name for a planned Apple Computer. In response, Apple changed the code name from "Carl Sagan" to "Butt-Head Astronomer." An offended Carl Sagan then sued. The court found in favor of the defendant, Apple Computer. *Contra*, *Flamm v. American Ass'n of University Women*, 201 F.3d 144 (2000) where an entry in a directory described one attorney, among other unflattering terms, as an "ambulance chaser."

[29] See, for example, *Paulson v. Ford Motor Co*. 614 N.W.2d 450 (Minn. App. 2000). The plaintiff in this matter was accused of sexual harassment by a lower-level employee. An employee from Ford's headquarters conducted an investigation and issued a report stating that the plaintiff had committed sexual harassment. The report also recommended that the plaintiff be demoted and transferred, which recommendation was followed by Ford. Shortly thereafter, the alleged victim of the harassment sued Ford, the plaintiff and another individual. The plaintiff then initiated this action, suing Ford and his accused for defamation and related claims. The trial and appellate courts concluded that the alleged defamatory statements contained in the report were privileged.

The defense of a "qualified privilege" may be lost if the employer "abuses" the privilege. If the defamation was made with malice, or in bad faith, the qualified privilege is lost. In addition, if assessments of an employee, communicated by a former employer to a prospective employer are not made in good faith, and/or are communicated to those who have no legitimate need to know, the qualified privilege is also considered abused and lost.

Were these the only threats to a business organization, the lives of human resource professionals everywhere would be much easier, and this article would end here. Unfortunately, it is not so.

III. PRINCIPLES OF FEDERAL PROSECUTION OF BUSINESS ORGANIZATIONS

As noted previously, civil litigation by employees and former employees are just some of the threats that a business organization faces. While a review of all the potential litigation threats to a business organization, from antitrust to water pollution violations, is far beyond the scope of this paper, human resource professionals should be aware of guidelines that the government considers when considering whether to prosecute a business and/or its employees.

As a result of high-profile lapses in legal compliance and ethical judgment by some notable companies, the government established guidelines that are to be considered by the U.S. Attorneys' office when considering prosecution. These guidelines serve several useful purposes. First, to ensure consistency in the prosecution of business organizations and to memorialize previously informal principles, the Department of Justice first issued the Holder Memorandum (Federal Prosecution of Corporations) in 1999. The document specified nine factors that prosecutors may consider when deciding whether to prosecute a business organization:

1. the nature and seriousness of the offense, including the risk of harm to the public, and applicable policies and priorities, if any, governing the prosecution of corporations for particular categories of crime;
2. the pervasiveness of wrongdoing with the corporation, including the complicity in, or condoning of, the wrongdoing by corporate management;
3. the corporation's history of similar conduct, including prior criminal, civil, and regulatory enforcement actions against it;
4. the corporation's timely and voluntary disclosure of wrongdoing and its willingness to cooperate in the investigation of its agents;
5. the existence and adequacy of the corporation's pre-existing compliance program;
6. the corporation's remedial actions, including any efforts to implement an effective corporate compliance program or to improve an existing one, to replace responsible management, to discipline or terminate wrongdoers, to pay restitution, and to cooperate with the relevant government agencies;
7. collateral consequences, including disproportionate harm to shareholders, pension holders and employees not proven personally culpable and impact on the public arising from the prosecution;
8. the adequacy of the prosecution of individuals responsible for the corporation's malfeasance; and
9. the adequacy of remedies such as civil or regulatory enforcement actions.

While the foregoing may seem unremarkable and present no obvious cause for concern among human resource professionals, this is hardly the case. Perhaps the most controversial factor for a prosecutor to consider is contained in a comment that notes, "….the completeness of its disclosure including, if necessary, a waiver of the attorney-client and work product protections, both with respect to its internal investigation and with respect to communications between specific officers, directors, and employees and counsel."[30] Almost needless to say, this issue arises only after a problem has occurred.

Also of interest was the document's statement that "[c]harging a corporation, however, does not mean that individual directors, officers, employees, or shareholders should not also be charged. Prosecution of a corporation is not a substitute for the prosecution of criminally culpable individuals within or without the corporation. Further, imposition of individual criminal liability on such individuals provides a strong deterrent against future corporate wrongdoing."[31]

Indeed, when considering whether to charge the business, as opposed to the employees, the Holder Memorandum specifically instructed prosecutors to evaluate the extent of the business' cooperation in the investigation. "In gauging the extent of the corporation's cooperation, the prosecutor may consider the corporation's willingness to identify the culprits within the corporation, including senior executives, to make witnesses available, to disclose the complete result of its internal investigation, and to waive the attorney-client and work product privileges."[32] The issue with regard to the waiver of the attorney-client privilege, as well as the issue of directors' and officers' (hereinafter "D&O") indemnification caused significant concern for business.

As part of that issue the document goes on to note that, "Another factor to be weighed by the prosecutor is whether the corporation appears to be protecting its culpable employees and agents. Thus, while cases will differ depending on the circumstances, a corporation's promise of support to culpable employees and agents, either through the advance of attorneys' fees, through retaining the employees without sanction for their misconduct, or through providing information to the employees about the government's investigation pursuant to a joint defense agreement, may be considered by the prosecutor in weighing the extent and value of a corporation's cooperation.

Although the Holder Memorandum noted that these were only "guidelines" it established a floor for even more aggressive approaches by the government, arguably in response to more, and far more serious, business scandals.

In January of 2003, the Thompson Memorandum[33] ("Principles of Federal Prosecution of Business Organizations") built on the Holder Memorandum. Although this document virtually restates the Holder Memorandum (although expanding the coverage to "business organizations" from "corporations") it represented a significant change. The Thompson Memorandum required prosecutors to actively weigh the noted factors, including, but not limited to, a business organization's payment of an employee's attorneys' fees as well as an organizations refusal to terminate a potentially-culpable employee in the decision to prosecute.

The Thompson Memorandum addressed three general issues. First was a concern that through D&O indemnification, a business would refuse to cooperate. The second was feigned

---

[30] Footnote two of the Holder Memorandum purports to limit this by noting, "This waiver should ordinarily be limited to the factual internal investigation and any contemporaneous advice given to the corporation concerning the conduct at issue. Except in unusual circumstances, prosecutors should not seek a waiver with respect to communications and work product related to advice concerning the government's criminal investigation."

[31] 1999 Holder Memorandum at 2.

[32] *Id*.at 5.

[33] Memorandum from Larry D. Thompson, Deputy Att'y Gen., to Heads of Dep't Components & U.S. Attorneys, on Principles of Federal Prosecution of Business Organizations (Jan. 20, 2003).

cooperation by a business. The third was a concern that a business would offer up one or more employees as sacrificial lambs in an effort to save itself.

The Thompson Memorandum addressed these concerns and noted, "The main focus of the revisions is increased emphasis on and scrutiny of the authenticity of a corporation's cooperation. Too often business organizations, while purporting to cooperate with a Department investigation, in fact take steps to impede the quick and effective exposure of the complete scope of wrongdoing under investigation. The revisions make clear that such conduct should weigh in favor of a corporate prosecution. The revisions also address the efficacy of the corporate governance mechanisms in place within a corporation, to ensure that these measures are truly effective rather than mere paper programs." The concern was rooted in reality.

Regardless, the government's approach was criticized. The harshest criticism seemed to be directed at the requirement that the corporation "cooperate in the investigation." This innocuous phrase was interpreted to require a business organization to:

1. waiver its attorney-client privilege and attorney work-product doctrine;
2. provide otherwise privileged internal documents to the government;
3. refuse to advance the attorneys' fees of individuals alleged to have committed the crime.

Then, in 2005, Acting Deputy Attorney General Robert D. McCallum, Jr. issued the McCallum Memorandum[34] ("Waiver of Corporate Attorney-Client and Work Product Protection.") This memorandum noted, in part, "…some United States Attorneys have established review processes for waiver requests that require federal prosecutors to obtain approval from the United States Attorney or other supervisor before seeking a waiver of the attorney-client privilege or work product protection. Consistent with this best practice, you are directed to establish a written waiver review process for your district or component." The memorandum also noted, "Such waiver review processes may vary from district to district (or component to component), so that each United States Attorney or component head retains the prosecutorial discretion necessary, consistent with their circumstances, to seek timely, complete, and accurate information from business organizations."

While this memorandum seemed to put a restriction on such requests, in an apparent attempt to address the concerns, it was criticized because it did not require uniform standards for prosecutors to seek a waiver and did not require that the standards be made publicly available. As a result it was argued that the memorandum would have little effect on such demands by prosecuting attorneys.

In response to continuing criticism, Deputy Attorney General Paul McNulty issued the McNulty Memorandum, revising certain aspects of the Thompson Memorandum. In particular, the McNulty Memorandum required that federal prosecutors seek a waiver of the attorney-client privilege, as well as the attorney work-product doctrine only in rare circumstances, and that such a request must be in writing and approved by the Deputy Attorney General.[35]

---

[34] Memorandum from Robert D. McCallum, Jr., Acting Deputy Att'y Gen., to Heads of Dep't Components & U.S. Attorneys, on Waiver of Corporate Attorney-Client and Work Product Production (Oct. 21, 2005).

[35] 2006 McNulty Memorandum at 9 ("Before requesting that a corporation waive the attorney-client or work product protections for Category I information [purely factual information relating to the underlying misconduct], prosecutors must obtain written authorization from the United States Attorney who must provide a copy of the request to, and consult with, the Assistant Attorney General for the Criminal Division before grating or denying the request.") see also id. at 10 (requiring that requests for "Category II" information consisting of attorney-client

In addition, any such request must also meet the "legitimate need test" consisting of a four-part test:

1. the likelihood and degree to which the privileged information will benefit the government's investigation;
2. whether the information sought can be obtained in a timely and complete fashion by using alternative means that do not require waiver;
3. the completeness of the voluntary disclosure already provided; and
4. collateral consequences to a corporation of a waiver. [36]

The McNulty Memorandum also backed down on the subject of attorneys' fees. Prosecutors could only take the advancement of attorneys' fees into account "[i]n extremely rare cases"[37] "when the totality of the circumstances show that it was intended to impede a criminal investigation…[indicating that] the corporation is acting improperly to shield itself and its culpable employees from government scrutiny.[38]

Nonetheless, prosecutors were still permitted to ask "[r]outine questions…"[39] such as "…how and by whom attorneys' fees are paid…[since such information] may be necessary to assess other issues, such as conflict-of-interest."[40]

In 2008, by way of the Filip Memorandum,[41] prosecutors could not "take into account whether a corporation is advancing or reimbursing attorneys' fees or providing counsel to employees, officers, or directors under investigation or indictment. Likewise, prosecutors may not request that a corporation refrain from taking such an action [to indemnify its employees]."[42] However, prosecutors could still ask questions about an attorney's representation of a corporation or its employees, officers, or directors, where otherwise appropriate under the law," and criminal obstruction of justice charges could apply, for example, 'if fees were advanced on the condition that an employee adhere to a version of the facts that the corporation and the employee knew to be false."[43]

The U.S. Attorneys' Manual has since been replaced by the Justice Manual.[44] The current Justice Manual provision on "Offering Cooperation: No Entitlement to Immunity" new as of August 2008, specifically states, "A corporation's offer of cooperation or cooperation itself does not automatically entitle it to immunity from prosecution or a favorable resolution of its case. A corporation should not be able to escape liability merely by offering up its directors, officers, employees, or agents. Thus, a corporation's willingness to cooperate is not determinative; that factor, while relevant, needs to be considered in conjunction with all other factors."[45]

---

communications or non-factual attorney work product be approved through ultimate written authorization of the Deputy Attorney General himself; and "[p]rosecutors are cautioned that Category II information should only be sought in rare circumstances.")

[36] 2006 McNulty Memorandum at 8.

[37] 2006 McNulty Memorandum at 11 n.3.

[38] *Id.*

[39] Id. at 12 n.4.

[40] Id.

[41] Memorandum from Mark Filip, Deputy Att'y Gen., to Heads of Dep't Components & U.S. Attorneys, on Principles of Federal Prosecution of Business Organizations (Aug. 28, 2008) [hereinafter 2008 Filip Memorandum].

[42] Id. at 13.

[43] Id.

[44] Available at https://www.justice.gov/jm/justice-manual

[45] Id. at § 9-28.740.

The foregoing is a brief description of the evolving rules that the government considers when deciding whether to prosecute a business organization, none of which are immutably carved in stone. As crime evolves so will the government's approach. Needless to say, society's- as well as the government's tolerance for noncompliance with legal and ethical responsibilities, whether such noncompliance is willful or not, has grown thin. Human resource professionals should keep in mind that while one of the goals of criminal prosecution and punishment is rehabilitation, the other goals, including punishment by way of fines and incarceration, are just as significant.

IV. RECOMMENDATIONS FOR HUMAN RESOURCE PROFESSIONALS

There are several significant issues that need to be addressed by an employer that may serve to reduce the likelihood of a lawsuit by an employee or former employee. Even more significant, these steps may reduce the likelihood of litigation, including criminal prosecution of the business organization, because of actions by employees. These steps begin even before an employee is hired.

A. Hiring

A reduction in the likelihood that a future employee may sue, or get the business organization sued, may be as simple as an adequate background check. The law requires that employers conduct a "reasonable" background check. What is "reasonable" depends on a variety of issues. As part of that all employers should require references and check with the references even though past employers should uniformly refuse to provide a reference.[46]

In times gone by, companies performed a background check to reduce the likelihood of employee theft. Presently, a background check may provide additional protection to a company from employees with a drug habit, a criminal record, or a potential for violence. A background check may also help a company reduce the risk from the loss of valuable trade secrets.

A background check may also reduce the rate of employee turnover, with the attendant cost of training new employees. A background check should include the following:

Civil lawsuits, bankruptcy filings and criminal convictions
Address verification
Verification of prior employment
Personal and professional references
Verification of educational claims

If a company offers an employee a company car or access to a company-owned vehicle, a background check with the department of motor vehicles should be performed. If a company were to put an employee with a drunk driving record into a company car, a lawsuit for negligent entrustment in the event of an injury-causing accident is almost certain. In other situations, usually high ranking executives, a company may also want to perform a post-employment lifestyle check.

In the absence of a conviction, a company should not ordinarily rely on arrest records. However, a company must also be careful about reliance on convictions. While a company may ordinarily rely on convictions when refusing to hire a candidate, as long as it is done in a

[46] Former employers should keep in mind that failing to disclose relevant information about a former employee's offenses may also result in a lawsuit.

nondiscriminatory manner, there are other limitations. The Equal Employment Opportunity Commission ("EEOC") recommends that an employer assure applicants that an accurate response will not automatically disqualify them from consideration.[47]

It is the EEOC's position that "blanket" rejection policies barring the employment of any applicant with a history of arrest or convictions are usually illegal under Title VII since such policies often disproportionately exclude members of certain racial or ethnic groups. If members of minority groups are disproportionately affected by policies concerning arrest or conviction records, the employer may continue its policy only if it can prove a business need. Only in very rare cases involving particularly sensitive positions have courts found that an employer has a business need for a blanket rejection policy.[48]

Therefore, as a general rule, the EEOC recommends that a decision to reject a particular applicant should be based on:

The nature and gravity of the offense;
The time since the conviction and/or completion of the sentence; and
The nature of the job held or sought.

Federal law may not be the only concern for employers. Some state laws may limit the use of arrest and conviction records by prospective employers.[49] The foregoing should make clear the necessity of a thorough background investigation. In addition, before hiring an applicant, an employer should schedule at least one interview with the applicant and at least one of the interviewers should be trained in interviewing.

V. DRUG LEGALIZATION AND EMPLOYER LIABILITY

The results of drug use and abuse in the workplace are well documented and include:

Premature death/fatal accidents
Injuries/accident rates
Absenteeism/extra sick leave
Loss of production
Tardiness/sleeping on the job
After-effects of substance abuse (hangover, withdrawal) affecting job performance
Impaired decision-making
Loss of efficiency
Theft
Lower morale of co-workers
Increased likelihood of trouble with co-workers/supervisors or tasks

[47] *See* EEOC Decision No. 80-26, n. 2.

[48] Hiring for the position of police officer would be such a situation. See, for example, *McCraven v. City of Chicago*, 109 F. Supp. 2d 935 (N.D. Ill. 2000) where the court held the use of arrest records as a blanket disqualification for all applicants for the position of police officer is lawful because of the "awesome responsibilities" of law enforcement.

[49] California, for example, has The Fair Chance Act, which went into effect on January 1, 2018, that generally prohibits employers with five or more employees from asking about an applicant's conviction history prior to a job offer.

Preoccupation with obtaining and using substances while at work, interfering with attention and concentration
Illegal activities at work including selling illicit drugs to other employees
Higher turnover
Training of new employees
Disciplinary actions[50]

These issues create a potential for both civil and criminal liability on the part of the employer as well as officers, directors and others in managerial positions.

Drug legalization presents several critical issues for employers. The Surgeon General's Report,[51] appropriately entitled "Facing Addiction in America" is the first of its kind on the subject of addiction, and noted the following:

The United States has a serious substance misuse problem. Substance misuse is the use of alcohol or drugs in a manner, situation, amount, or frequency that could cause harm to the user or to those around them. Alcohol and drug misuse and related substance use disorders affect millions of Americans and impose enormous costs on our society. In 2015, 66.7 million people in the United States reported binge drinking in the past month and 27.1 million people were current users of illicit drugs or misused prescription drugs. The accumulated costs to the individual, the family, and the community are staggering and arise as a consequence of many direct and indirect effects, including compromised physical and mental health, increased spread of infectious disease, loss of productivity, reduced quality of life, increased crime and violence, increased motor vehicle crashes, abuse and neglect of children, and health care costs. The most devastating consequences are seen in the tens of thousands of lives that are lost each year as a result of substance misuse. Alcohol misuse contributes to 88,000 deaths in the United States each year; 1 in 10 deaths among working adults are due to alcohol misuse. In addition, in 2014 there were 47,055 drug overdose deaths including 28,647 people who died from a drug overdose involving some type of opioid, including prescription pain relievers and heroin—more than in any previous year on record.

Needless to say, substance abusers/misusers are not doing so exclusively in the privacy of their home during their time off from work. Although the Surgeon General's Report does not address the wisdom of legalization, it specifically states, "Although this Report does not examine the issue of marijuana legalization, its continually evolving legal status is worth mentioning because of implications for both research and policy. As mentioned elsewhere, marijuana is the most commonly used illicit drug in the United States, with 22.2 million people aged 12 or older using it in the past month. In recent years marijuana use has become more socially acceptable among both adults and youth, while perceptions of risk among adolescents of the drug's harms have been declining over the past 13 years. (Citations omitted).[52]

Other statements in the report, related to the subject of drug legalization, provide food for thought. Even though the United States spends more than any other country on health care, it ranks 27th in life expectancy, which has plateaued or decreased for some segments of the population at a time when life expectancy continues to increase in other developed countries—and

[50] The National Council on Alcoholism and Drug Dependence, Inc. Available at: https://ncaddnational.org/addiction_articles/drugs-and-alcohol-in-the-workplace/
[51] U.S. Department of Health and Human Services (HHS), Office of the Surgeon General, Facing Addiction in America: The Surgeon General's Report on Alcohol, Drugs, and Health. Washington, DC: HHS, November 2016. Available at https://www.hhs.gov/sites/default/files/facing-addiction-in-america-surgeon-generals-report.pdf
[52] Id. at 1-20.

the difference is largely due to substance misuse and associated physical and mental health problems."[53]

For business the results of legalization, as well as the government's efforts to insulate users and misusers from on-the-job discipline, as well as criminal prosecution, are devastating and expensive. Substance misuse and abuse disorders also have serious economic consequences, costing more than $400 billion annually in crime, health, and lost productivity…. Alcohol misuse and alcohol use disorders alone costs the United States approximately $249 billion in lost productivity, health care expenses, law enforcement, and other criminal justice costs. The costs associated with drug use disorders and use of illegal drugs and non-prescribed medications were estimated to be more than $193 billion in 2007.[54]

The foregoing broad generalities are instructive. On a more practical level, business must be alert to specific issues related to alcohol and drug use. Arguably the most significant issue for business, and potentially the most expensive, is driving under the influence.

As part of that the Surgeon General's report notes, "DUI continues to be among the most frequent causes for arrests every year. But at approximately 1.3 million per year, these arrests represent only about 1 percent of the actual alcohol-impaired driving incidents reported in national surveys, suggesting that there are many more people who drive while impaired that have not been arrested, putting themselves and others at high risk of being harmed."[55]

In addition, marijuana use can also impair driving skills. While estimates vary, marijuana is linked to a roughly two-fold increase in accident risk and that risk is compounded when marijuana is used with alcohol.[56]

Business should not assume that all such issues arise only on an employee's personal time. In addition, the report specifically notes that the statistics only account for alcohol-related driving impairment and fail to measure other impairing substances.[57] "A study by NHTSA" (the National Highway Traffic Safety Administration) "tested oral fluid and blood specimens from a random sample of drivers at the roadside (during daytime on Friday or nighttime Friday to Sunday) and found 12 to 15 percent had used one or more illegal substances. Drivers tested positive for drugs in approximately 16 percent of all motor vehicle crashes."[58]

"Opioid analgesic pain relievers are now the most prescribed class of medications in the United States, with more than 289 million prescriptions written each year. The increase in prescriptions of opioid pain relievers has been accompanied by dramatic increases in misuse…and by a more than 200 percent increase in the number of emergency department visits from 2004 to 2011."[59]

The report goes on to note that "[a]lmost 8 percent of the population met diagnostic criteria for a substance use disorder for alcohol or illicit drugs, and another 1 percent met diagnostic criteria for both an alcohol and illicit drug use disorder."[60] Unfortunately, "[a]lthough 20.8 million people (7.8 percent of the population) met the diagnostic criteria for a substance use disorder in 2015, only 2.2 million individuals (10.4 percent) received any type of treatment."[61]

---

[53] Id. at 1-1
[54] Id.at 1-2
[55] Id. at 1-13
[56] Id. at 1-21
[57] Id.
[58] Id. at 1-13-14
[59] Id. at 1-14
[60] Id. at 1-7
[61] Id.

Among the questions created by drug legalization for business are:

1. Will legalization lead to an increase in addiction?
2. Will legalization result in increased drug use, whether on or off the job, with the potential that employees will either use drugs at work or be under the influence at work?
3. Will legalization result in an increase in drug-related workplace issues including, but not limited to, sexual harassment, accidents, absenteeism, reduced efficiency and violence?

While there are studies that show an increase in "use and abuse"[62] which the Surgeon General's Report seems to support, studies that specifically address the issue of an increase in addiction are difficult to locate. While studies tend to indicate that an increase in addiction is not necessarily a result of legalization, at least until recently, the evidence was limited.[63] Although the issue of addiction, with its effects on the employer's workplace and insurance premiums, among other issues, is significant, it is not the only concern. For employers it may not even be the most important question. For employers legalization presents two additional significant issues.

A. *Will legalization result in increased use?*

And for that, the answer is, unfortunately, yes. As the Surgeon General's Report notes, use is becoming more socially acceptable.[64] As part of that, business must then consider whether legalization will result in an increase in other related workplace issues including, but not limited to workplace sexual harassment, absenteeism, reduced efficiency and violence, among other issues.

And while the report does not specifically address workplace violence, it does discuss intimate partner violence, sexual assault, and rape noting, "[t]hese crimes happen to both women and men and are often associated with substance use."[65] Admittedly, while there is a high correlation between substance use and intimate partner violence, this does not mean that substance use is the cause of the violence.[66]

As a result of the foregoing, for business it means that all applicants should be required to take a drug test by a qualified drug testing laboratory unless prohibited by state law or a collective bargaining agreement.[67] In addition to the standard reasons for drug testing, employers should be aware that substance abusers are more likely to be involved in sexual harassment, at least in part

---

62 See, e.g., Impacts of recreational cannabis legalization on cannabis use: a longitudinal discordant twin study. Addiction, Volume 118, Issue One, January, 2023, pages 110-118 available at https://onlinelibrary.wiley.com/doi/10.1111/add.16016 noting an average 20% increase in use.

63 See, e.g., Laura L. Hirschfeld, Legal Drugs? Not Without Legal Reform: The Impact of Drug Legalization on Employers Under Current Theories of Enterprise Liability, 7 Cornell J.L. & Pub. Pol'y 757,773 (1998).

64 Surgeon General's Report, *supra*., at 1-20

65 Id.

66 Id.

67 See, for instance, "passyourdrugtest.com." This site provides information about every drug test available and allows users to post information about companies and their drug testing policies. This site also lists the various drugs and how long traces of the drugs remain in a person's system. The site offers various products to assist users in passing drug tests and thoughtfully provides a money back guarantee in the event that a product fails to work as advertised.

because of their lowered level of inhibition, creating potential liability on the part of the employer.[68] Users of high-risk drugs are also likely to be involved in violence, discrimination as well as be at risk for mental health problems and suicide.[69]

For business, the concern is that the victim of the harassment, or violence, may be able to sue the employer, the "deep pocket" as well as the harasser or perpetrator. In some situations the end result may be criminal prosecution of not only the perpetrator, but other managerial individuals that were aware of the drug use and did nothing about it.

Allegations of harassment should be addressed by way of a "reasonable" investigation. If the alleged harasser is terminated, it is not unheard of for them to sue the company for wrongful termination. And, if the alleged harassment was fabricated, for instance as a result of a personal vendetta, the terminated employee may have a valid suit for wrongful termination. While the plaintiff in that situation may also have a valid suit for defamation, and possibly other grounds as well against the accuser, it is the employer, again, that is the "deep pocket."

There is another significant issue that is not addressed by the Surgeon General's report. While the Surgeon General's report addresses legal drugs, such as alcohol and, in some states marijuana, as well as illegal drugs, it ignores another serious threat. A drug that at least at the present, is flying under the radar. While the hazards that exist with legal drugs as well as illegal drugs are well-known, employers should also be aware of the threat that is presented by anabolic steroids.[70] Unfortunately, it is difficult to estimate the prevalence of steroid misuse in the United States because many national surveys on the subject of drug use do not include questions about steroids.[71]

Originally, use and abuse of steroids was limited to athletes. Although it was not the first legislation on the subject,[72] Congress recognized the problem by way of the 1990 Anabolic Steroids Control Act. The Department of Justice Office of Justice Programs had this to say about the law in 1995:

> The Anabolic Steroid Control Act of 1990 placed more than two dozen anabolic steroids into the Controlled Substances Act. Although there is evidence of considerable achievement, abuse of anabolic steroids is a significant threat to the

[68] See, e.g., Int J Environ Res Public Health, 2022 Nov; 19(22): 15090. Published online 2022 Nov 16 doi: 10,3390/ijerph192215090, "Sexual harassments Related to Alcohol and Drugs Intake: The Experience of the Rape Centre of Turin.

[69] CDC.gov

[70] Anabolic steroids are a Schedule III controlled substance under 21 U.S.C. § 812. Under 21 U.S.C. § 841(b)(1)(D), any person who knowingly or intentionally trafficks in, or possesses with intent to traffic in, a Schedule III controlled substance shall be sentenced to a term of imprisonment of not more than 5 years, or if the person committed the offense after a prior conviction for a felony drug offense has become final, not more than 10 years imprisonment. The statutory maximum may double if the person distributes the drug to persons under the age of 21, or distributes or manufactures the drug in or near schools and colleges

[71] NIDA. 2024, July 11. Anabolic Steroids and Other Appearance and Performance Enhancing Drugs (APEDs). Retrieved from https://nida.nih.gov/research-topics/anabolic-steroids on 2024, July 17

[72] The first major legislation regulating steroids was the Anti-Drug Abuse Act of 1988 that changed the penalty for the illegal distribution of steroids from a misdemeanor to a felony. Anti-Drug Abuse Act of 1988, Pub. L. No. 100-690, 102 Stat. 4181 (amended 1990).

general public health and safety, especially with respect to adolescents and young adults.[73]

Then, in 2004 Congress passed the Anabolic Steroid Control Act of 2004[74] to "…address the abuse of steroids by athletes and, especially, by youngsters and teenagers."[75] An article from 2007 notes , "… a major shift in steroid and performance-enhancing drug abuse is occurring, and the next place it emerges will be in the workplace."[76] "What are the consequences if employees choose to abuse steroids on their own time for improved strength or body image? What impact does that have on the workplace? Presently, the answer to that question is unknown because steroids are not tested in the non-sports workplace, nor are there studies surveying workplace steroid abuse. However, experts in this area estimate there are between 1 million and 3 million former or current abusers of steroids in the United States. Also, there are compelling studies suggesting the abuse of steroids approaches 10 percent of high school males and females as young as 13 years old and that steroids are being abused by young adults who are not professional athletes. These studies were done a few years ago, which suggests those high-school steroid users who are not in professional sports are now in the workplace."[77]

Although Congress addressed the issue of steroid use and abuse, the legislation was intended to apply to athletes. "Steroids are now Schedule III controlled substances as a result of the passage of the 1990 Anabolic Steroid Control Act, and persons dealing or abusing them would face the same penalty as those who are dealing with cocaine, heroin, or methamphetamine. They are illegal to possess or use without a doctor's prescription…."[78]

Individuals who abuse steroids are more likely to engage in violence as well as other high-risk behaviors, such as substance abuse, smoking, and binge drinking.[79]

Violence is not the only issue associated with the use/abuse of steroids, although the use of steroids, alone, may not be the cause of the violence. There is some evidence that use of steroids may be associated with the use of other drugs of abuse and may serve, for some users, as a gateway/introductory drug to use of other controlled substances.[80]

Employers should be aware that anabolic steroid users are more likely to use drugs such as marijuana, prescription opioids, cocaine or heroin.[81] In addition, steroid use and abuse is associated with high risk behaviors. "…individuals who abuse steroids are more likely to engage in other high-risk behaviors, such as substance abuse, smoking, violent behaviors, and binge drinking These high-risk behaviors are probably due to some underlying psychiatric disorder that is

---

[73] Conference on the Impact of National Steroid Control Legislation in the United States. NCJ Number 163342. 1995. Available at https://www.ojp.gov/ncjrs/virtual-library/abstracts/conference-impact-national-steroid-control-legislation-united

[74] Anabolic Steroid Control Act of 2004, Pub. L. No. 108-358, 118 Stat. 1661 (2004).

[75] 150 Cong. Rec. S10608 (daily ed. Oct. 6, 2004) (statement of Sen. Joseph Biden).

[76] Id. at 4.

[77] Steroids on the Job: An Emerging problem. August 8, 2007. Occupational Safety and Health. https://ohsonline.com/Articles/2007/08/Steroids-on-the-Job-An-Emerging-Problem.aspx?Page=1

[78] Id.at 4

[79] https://ohsonline.com/Articles/2007/08/Steroids-on-the-Job-An-Emerging-Problem.aspx#:~:text=Another%20significant%20finding%20is%20that,these%20are%20undesirable%20workplace%20behaviors.

[80] 2006 Steroids Report Prepared by the Steroids Working Group United States Sentencing Commission, March 2006. https://www.ojp.gov/ncjrs/virtual-library/abstracts/steroids-report-2006

[81] NIDA. 2024, July 11. Anabolic Steroids and Other Appearance and Performance Enhancing Drugs (APEDs). Retrieved from https://nida.nih.gov/research-topics/anabolic-steroids on 2024, July 16

amplified by the abuse of steroids. In the extreme, these behaviors exacerbated by steroid abuse have been associated with at least 20 murders caused by "roid rage" in the United States alone."[82]

For the foregoing reasons drug testing, including tests for the presence of anabolic steroids, where allowed by law and collective bargaining agreements are a necessity and should not end with job applicants. All companies should establish a policy on drug testing.[83] The policy should be reasonable in scope and uniformly applied to all employees.

VI. CRIMINAL LAW IMPLICATIONS FOR EMPLOYERS

While civil lawsuits are traditionally the primary reason for employers to carefully screen their applicants, there is yet another reason of at least equal importance. Corporate scandals involving Honda, Enron, Arthur Andersen and Martha Stewart, among numerous others, have given rise to criminal prosecutions. This is yet another reason for employers to carefully screen all applicants. In certain situations, an employer may need to perform a background check on existing employees, if such a check was not performed previously.

In addition, an employer must also have a program in place to prevent and report criminal activity. Federal sentencing guidelines for corporations allow dramatic reductions in fines and penalties for companies with an internal program to prevent and report criminal behavior. Corporate directors that fail to set up management systems promoting lawful behavior may be held personally liable for fines,[84] and thus face both criminal and civil liability.

Chapter 8 of the United States Sentencing Commission Guidelines Manual lists seven "minimum steps" that employers should take:

- Establish Compliance standards and procedures for employees that are reasonably capable of reducing criminal acts. Such policies should contain broad expressions on honesty, integrity and fairness, possibly along with examples on gifts, entertainment and bribes.
- Assign Responsibility for overseeing the program to high-level personnel.

Assigning responsibility to a lower-level employee conveys the impression that upper management does not consider the program to be important. As part of that, employers must exercise due care not to delegate substantial discretionary authority to persons who are prone to engage in criminal behavior. This ordinarily requires a reasonable background check.

Take reasonable steps to communicate standards and procedures to all employees. Take reasonable steps to achieve compliance with standards by using monitoring and auditing systems

---

[82] Id. at 3.

[83] For companies that are unionized, this policy may be established by the collective bargaining agreement.

[84] See, for instance*, In re Caremark Int'l, Inc*. Derivative Litig. 698 A.2d 959 (Delaware, 1996) where the court noted the vigilance required of a director in a modern corporation. The court observed that directors have a duty to assure "…that information and reporting systems exist in the organization that are reasonably designed to provide to senior management and to the board itself timely, accurate information sufficient to allow management and the board, each within its scope, to make informed judgments concerning both the corporation's compliance with law and its business performance."
In referring to the *Federal Sentencing Guidelines for Organizations*, the court stated, "A director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists." Therefore, the absence of an effective internal compliance program may create personal liability on the part of directors in shareholder derivative suits.

designed to detect lawbreaking and by having in place multiple reporting systems that employees can use to report criminal conduct, including, but not limited to hotlines. As part of this the company must establish and enforce a policy that forbids retaliation against employees. In addition, employers should:

Consistently enforce reasonable standards using appropriate disciplinary mechanisms and, as appropriate, disciplining individuals responsible for failure to detect an offense. Assure that the punishment fits the crime. Although all offenses must be handled on a case-by-case basis, take reasonable steps to assure uniformity.

Immediately after an offense has been detected, respond appropriately and take reasonable steps to prevent further similar offenses. Notify the appropriate authorities immediately and do not attempt to conceal the offense. Take steps to keep employees reasonably informed.

VII. CONCLUSION

For business the most important subject is education and monitoring of employees. As part of that, employer's should be aware that the Affordable Care Act requires the majority of United States health plans and insurers to offer prevention, screening, brief interventions, and other forms of treatment for substance abuse disorders."[85]

Reducing the likelihood that an employer will need to terminate an employee reduces the likelihood that an employer will be sued for wrongful termination. While there are some situations requiring layoffs that are beyond the control of employers, such as economic downturns, there are many factors that an employer can, and should control, to minimize the likelihood of a lawsuit.

While an employer that shows a concern with fairness in the discipline/termination process may be viewed by a court as having abandoned employment-at-will, as commentators have noted, employees' perception of the fairness of the employer's discipline/termination process is also a significant factor affecting an employee's likelihood of filing a lawsuit.[86] Thus, while eliminating a risk of a lawsuit is impossible, reasonable steps will reduce the likelihood of a civil lawsuit and, if a lawsuit is filed, improve the chances that the employer will prevail. Perhaps more importantly, reducing the likelihood of a civil lawsuit may also reduce the likelihood of criminal prosecution of the employer.

That, alone, however, is insufficient. Organizations with a cavalier attitude toward legal compliance face a risk that cannot be overstated. The Holder Memorandum specifically states, "Charging a corporation for even minor misconduct may be appropriate where the wrongdoing was pervasive and was undertaken by a large number of employees or by all the employees in a particular role within the corporation…. or was condoned by upper management. On the other hand, in certain limited circumstances, it may not be appropriate to impose liability upon a corporation, particularly one with a compliance program in place…. for the single isolated act of a rogue employee."[87]

All of the noted memoranda also include the following, "Of these factors, the most important is the role of management. Although acts of even low-level employees may result in criminal liability, a corporation is directed by its management and management is responsible for a corporate culture in which criminal conduct is either discouraged or tacitly encouraged. As stated

[85] Id. at 1-20

[86] See, for instance, Gillespie, T. and Parry, R., 2006. "Fuel for Litigation? Links between Procedural Justice and Multisource Feedback." Journal of Managerial Issues, 4: 530-546.

[87] The later Thompson and McNulty Memoranda repeat this language. Justice Manual § 9-28.500.

in commentary to the Sentencing Guidelines: Pervasiveness [is] case specific and [will] depend on the number, and degree of responsibility, of individuals [with] substantial authority… who participated in, condoned, or were willfully ignorant of the offense. Fewer individuals need to be involved for a finding of pervasiveness if those individuals exercised a relatively high degree of authority. Pervasiveness can occur either within an organization as a whole or within a unit of an organization."

While criminal prosecution may be the greatest threat, although much less likely, the danger that civil litigation represents should not be underestimated. In either case, the cost of defending one, or both such actions, may be ruinous to a company.

WHEN CHEATING GOES DIGITAL: LEGAL HURDLES IN PROTECTING ACADEMIC INTEGRITY

MELISSA BALDO[*]
MARLEEN SWERDLOW[**]
MELANEY WHITING[***]

ABSTRACT

Students cheating and educators trying to prevent them from doing so has been an ongoing battle since time immemorial. However, the modern methods students are using have shifted from the classroom to the courtroom. Many in academe are unaware of this new dynamic and the legal hurdles they will encounter once they become informed and try to navigate through them. This paper will examine two such legal impediments to academic integrity. First, U.S. copyright law as amended by the Digital Millennial Copyright Act (DMCA) will be explored in terms of the work product of university professors being posted to online service platforms without their knowledge or permission. One such platform, Course Hero, will be closely examined to serve as a case study of the predicament presented by the DMCA and the labyrinth that online service providers can create to obstruct a takedown. Second, this paper will delve into a student's attempt to use the shield of the Fourth Amendment as a sword to block online proctoring which serves to maintain academic integrity.

I. INTRODUCTION

The greatest college cheating scandal that ever occurred is not Lori Loughlin and other celebrities who bribed their children's way into college. Instead, it is the rampant cheating that occurs every day within the halls of academe. It used to be that the greatest concern for professors was to be sure that students were not looking at another person's exam. Who knew that one day they would yearn for the simplicity of those cheating methods? The small cheating fires that used to occur have become a technological wildfire with the advent of ChatGPT, Course Hero, and other platforms.

According to one shocking poll by Kessler International, a digital forensics firm, eighty-six percent of college students surveyed admitted to cheating.[1] Of those surveyed forty-two percent admitted to purchasing custom term papers, essays, and thesis online, twenty-eight percent

---

[*]J.D., Assistant Professor of Business Law, Lamar University, Beaumont, Texas
[**]J.D., Professor of Business Law, Lamar University, Beaumont, Texas
[***] J.D., Instructor of Business Law, Lamar University, Beaumont, Texas
[1] Karen Farkas, *86% of College Students Say They've Cheated, It's Easier Than Ever with Mobile Devices*, CLEVELAND,COM (Feb. 7, 2017), https://www.cleveland.com/metro/2017/02/cheating_in_college_has_become.html.

admitted to using a service to take their online classes for them, and seventy-two percent admitted to using their phone, tablet, or computer to cheat in class.[2] It appears that cheating has become the norm and digital tools are the du jour choice of dishonest students. The tools to aid them with their ethical downslide have become more prolific since the burgeoning internet and the emergence of accessible artificial intelligence, such as ChatGPT.

Chat GPT is a large language model (LLM) which uses deep learning to generate human-like text based on prompts from its users. An LLM is "a computer algorithm that processes natural language inputs and predicts the next word based on what it's already seen."[3] It is able to do this because it has been trained using deep learning.[4] This method uses large labeled data sets which enable a computer to learn by example.[5] It is similar to a parent teaching a toddler what a dog is through positive or negative reinforcement.[6] This very smart chatbot has made AI accessible to the common man, and its introduction on the world stage has been explosive. Everyone is using it, including students who prefer to take the easy route to writing papers and completing homework assignments. And they are willing to fight for the right to do it.

It did not take long for the ChatGPT landscape to become marred by litigation. A student in Massachusetts has already sued Higham High School (HHS) for penalizing him for using ChatGPT to research and do his outline for an assignment.[7] The facts reveal that all high school juniors at HHS are given an extensive writing assignment designed to teach them how to conduct primary and secondary source research.[8] Instructions regarding the importance of maintaining academic integrity were emphasized by the teacher, and a one-page document was provided to students that detailed how to use AI properly.[9]

---

[2] *Id.*

[3] Lucas Mearian, *What Are LLMS, and How Are They Used in Generative AI?* COMPUTERWORLD (Feb. 7, 2024), https://www.computerworld.com/article/3697649/what-are-large-language-models-and-how-are-they-used-in-generative-ai.html.

[4] Kinza Yasar & Alexander S. Gillis, *What is Deep Learning and How Does it Work?* TECHTARGET (Sept. 23, 2024), https://www.techtarget.com/searchenterpriseai/definition/deep-learning-deep-neural-network.

[5] *Id.*

[6] *Id*.

[7] Harris v. Adams, 757 F.Supp.3d 111 (D. Mass. 2024).

[8] *Id*. at 123.

[9] *Id.* A one-page document given to students which was referenced as "HHS' written expectations on Academic Dishonesty and use of AI" contained the following information:

> The "Artificial Intelligence (A.I.) & Chatbots" section of the document instructs students not to use AI for assignments "unless explicitly permitted and instructed," as AI tools should not be used to "*replac*[*e*] [the students'] own critical thinking." (citation omitted) (emphasis in original). It explicitly states that, "[i]f there is a question about when, where, and how to use these tools, the student *must* communicate with their instructor in advance of use." (citation omitted) (emphasis in original). The document stresses that students must "[g]ive credit to AI tools whenever used, even if only to generate ideas or edit a small section of student work." (citation omitted) The written expectations also spell out that when students use AI to complete an assignment, they must create:
>
> > [A]n appendix for every use of AI showing: (a) the entire exchange, highlighting the most relevant sections; (b) a description of precisely which AI tools were used . . . (c) an explanation of how the AI tools were used . . . ; (d) an account of why AI tools were used (e.g. procrastination, to surmount writer's block, to stimulate thinking, to manage stress

When Turnitin.com flagged a portion of the student's work as being generated by AI, the teacher investigated further using Chrome's Revision History tool.[10] The tool allows users to determine "how many edits students made to their essays, how long students spent writing, and what portions of the work were copied and pasted."[11] The teacher discovered that the student had only spent fifty-two minutes in the document compared to his classmates, who had spent between seven and nine hours in their documents.[12] Additionally, the teacher found several books cited in the student's work that do not exist.[13] The student's attorney argued that there was no specific AI policy in the student handbook and that getting help from AI to research and create an outline was not cheating.[14] The federal magistrate was not persuaded and denied the request for a temporary injunction.[15] In the past, allowing a friend to do one's work would have been a clear-cut case of cheating. The only difference in the present situation is that the friend's name is ChatGPT.

This digital deception by students has led many universities, such as UNC Chapel Hill, Pepperdine, University of Florida, Cornell University, and many others, to utilize AI detection tools to try to identify those who are cheating.[16] However, caution should be exercised as AI detection tools are far from perfect. The error rate can be as high as twenty percent, which is unsettling considering the ramifications that follow an accusation of a breach of academic integrity.[17] One can already feel the barrage of lawsuits being prepared now by disgruntled students claiming a false positive. Perhaps the focus of academe should be on creating a culture of academic integrity until foolproof AI detection software is available.

Before students get too enamored with the prospect of ChatGPT completing their assignments, they should recognize ChatGPT's inclination to hallucinate on random occasions without rhyme or reason.[18] In other words, it makes things up. Perhaps AI is sentient after all, and it has a wicked sense of humor. Two New York attorneys were not amused, however, when

---

level, to address mismanagement of time, to clarify prose, to translate text, to experiment with the technology, etc.). (citation omitted) *Id.* at 122-23.

[10] *Id.* at 124.

[11] *Id*.

[12] *Id.* at 125.

[13] *Id*.

[14] *Id*. at 122.

[15] *Id.* at 145. *See also* Carol Britton Meyer, *Judge Denies Motion for Preliminary Injunction in AI Case Involving Hingham Student; Attorney Says Case Will Continue,* ANCHOR (Nov. 22, 2024), https://www.hinghamanchor.com/judge-denies-motion-for-preliminary-injunction-in-ai-case-involving-hingham-student-attorney-says-case-will-continue/.

[16] *AI detector by JustDone*, JUSTDONE, https://justdone.com/ai-detector?utm_source=bing&utm_medium=cpc&utm_campaign=485848552&utm_content=1233653131799896&utm_adset_id=1233653131799896&utm_term=justdone.com&utm_network=o&utm_matchtype=b&msclkid=d9c4db89129b1dfa49d7b3d8c028c980 (last visited June 17, 2025).

[17] Victor Tangermann, *There's a Problem With That App That Detects GPT-Written Text: It's Not Very Accurate*, FUTURISM (Jan. 9, 2023, 2:32 PM EST), https://futurism.com/gptzero-accuracy.

[18] Anosha Shariq, *ChatGPT Hallucinations are Getting Worse--and Even OpenAI Doesn't Even Know Why,* ALLABOUTAI.COM (May 8, 2025), https://www.allaboutai.com/ai-news/chatgpt-is-making-more-mistakes-and-even-openai-doesnt-know-why/.

they were chastised by a judge for citing six case citations in a brief generated by ChatGPT that were completely fabricated.[19] Neither of them knew about ChatGPT's penchant for whimsy.

II. COURSE HERO

Perhaps the most insidious nemesis that professors face is due to the birth and proliferation of online platforms designed to "assist" students. Although they sound innocent enough, a close examination reveals the dark underbelly that is a scourge to unsuspecting professors everywhere. Course Hero is one such online platform and will serve as the case study to illustrate the problem.

Course Hero was founded in 2006 by college student Andrew Grauer as an online learning platform for course-specific study resources. Course Hero is designed "to help students graduate confident and prepared."[20] The question is: prepared for what? If Course Hero means prepared to tackle future problems and responsibilities in the workplace and society ethically, they may want to revisit their business model. Course Hero is set up so that anyone can initially do a free search for a particular university and course to get a sampling of the documents that have been uploaded to see whether they might be advantageous to the searcher. There usually is nothing to identify the individual who uploaded the documents nor is there any discernible mechanism to verify whether the uploader was the author of the material. Viewers are teased with either small print or blurred segments. If they want to see the full document that piques their interest, they must pay the membership fee to gain full access. However, the monthly cost can be mitigated and even eliminated by uploading course documents because the more viewers load, the less they pay. This adds to the Course Hero treasure trove and is quite clever because the more documents on the site, the more users it will attract.[21] Given that Course Hero was valued at over one billion dollars in 2020, Course Hero's plan is working.[22] Unfortunately, this largess is due in part to the unauthorized uploading and posting of the work product of university professors, which makes one wonder if professors can sue Course Hero for such blatant copyright infringement. To ascertain the answer, it becomes necessary to examine copyright law. Copyright law is complex and multi-faceted, so this paper's foray will be somewhat cursory and framed in terms of the work product of professors whose work is being published and sold on Course Hero.

---

[19] Sara Merken, *New York Lawyers Sanctioned for Using Fake ChatGPT Cases in Legal Brief*, REUTERS (June 26, 2023), https://www.reuters.com/legal/new-york-lawyers-sanctioned-using-fake-chatgpt-cases-legal-brief-2023-06-22/.

[20] Matt Russoniello, *How Does Course Hero Work?,* COURSE HERO (Oct. 16, 2018), https://www.coursehero.com/blog/how-does-course-hero-work/.

[21] *Uploads for Unlocks,* COURSE HERO, https://support.coursehero.com/hc/en-us/articles/205142820-Uploads-for-Unlocks, (last visited June 17, 2025).

[22] Tony Wan, *With $1.1B Valuation, Course Hero Joins the Edtech Unicorn Stable*, EDSURGE (Feb. 12, 2020), https://www.edsurge.com/news/2020-02-12-course-hero-joins-the-edtech-unicorn-stable.

III. COPYRIGHT PROTECTION

A copyright is a type of intellectual property that protects original works of authorship as soon as an author fixes the work in a tangible form of expression.[23] In other words, as soon as an exam, discussion board, or assignment is created by a professor, copyright protection exists as long as it is an original work and was not copied from a test bank or other source. It must be an original product of the professor's mind. Many have the misconception that copyrights can only be achieved by filing with the U.S. Copyright Office, but this is not the case. Copyright protection is immediate upon the creation of the work into a tangible form of expression.[24] Copyright ownership may vary depending on the policy of a particular university and whether outside funding, such as grants, is involved.[25]

Although filing with the U.S. Copyright Office is not required to have copyright protection, there are clear advantages in doing so. The most significant advantage is that filing is a necessary prerequisite before the owner can bring a copyright infringement suit in federal court or be eligible for statutory damages or attorneys' fees.[26] Since most lawsuits are about money, being barred from the right to statutory damages might defeat the purpose of the lawsuit. Therefore, registering one's work product with the U.S. Copyright Office within three months of publication, or before infringement of the work, is wise to do.[27] Although a copyright has been created, this does not mean it is safe from infringement. Infringement in the legal realm refers to the unauthorized use of protected material.[28] The essential question is: When Course Hero and other such sites infringe upon a professor's copyright, can a professor sue for copyright infringement? To answer this question, a further examination into the law surrounding copyright is necessary.

IV. THE DIGITAL MILLENIUM COPYRIGHT ACT

U.S. copyright law was amended in 1998 by the passage of the Digital Millennium Copyright Act (DMCA), which was signed into law by President Clinton.[29] Specifically, "Title II, the 'Online Copyright Infringement Liability Limitation Act,'" creates limitations on the liability of online service providers for copyright infringement when engaging in certain types of activities."[30] The updates to copyright law are:

---

[23] Copyright Act, U.S.C. § 102 (1976).

[24] *Copyright Basics*, USPTO, https://www.uspto.gov/ip-policy/copyright-policy/copyright-basics (last visited June 17, 2025).

[25] Lindsey Gumb & William Cross, *In Keeping with Academic Tradition: Copyright Ownership in Higher Education and Potential Implications for Open Education*, 5(1) J. OF COPYRIGHT IN EDUC. & LIBRARIANSHIP 1, 5 (Apr. 25, 2022).

[26] *Benefits of Copyright Registration,* COPYRIGHT ALLIANCE, https://copyrightalliance.org/education/copyright-law-explained/copyright-registration/benefits-of-copyright-registration/ (last visited June 17, 2025).

[27] Gene Markin, *What You and Your Business Need to Know About Copyright Law and Infringement*, Nat'l L. Rev. (June 29, 2020), https://www.natlawreview.com/article/what-you-and-your-business-need-to-know-about-copyright-law-and-infringement.

[28] Ty McDuffy, *What Is Infringement?* LEGAL MATCH LAW LIBRARY (Apr. 19, 2022), https://www.legalmatch.com/law-library/article/what-is-infringement.html.

[29] U.S. Copyright Office Summary*, The Digital Millennium Copyright Act of 1998* (Dec. 1998), https://www.copyright.gov/legislation/dmca.pdf.

[30] *Id.*

> (1) establishing protections for online service providers in certain situations if their users engage in copyright infringement, including by creating the notice-and-takedown system, which allows copyright owners to inform online service providers about infringing material so it can be taken down; (2) encouraging copyright owners to give greater access to their works in digital formats by providing them with legal protections against unauthorized access to their works (for example, hacking passwords or circumventing encryption); and (3) making it unlawful to provide false copyright management information (for example, names of authors and copyright owners, titles of works) or to remove or alter that type of information in certain circumstances.[31]

If an individual is a copyright owner, he has the exclusive right to reproduce, distribute, sell, or display his work product *subject to certain statutory limitations*.[32] These statutory limitations are the loophole upon which Course Hero and other such websites rely. The limitations derive from the DMCA, which was enacted to protect copyright holders from online theft via the unlawful reproduction or distribution of their works.[33] "The DMCA covers music, movies, text, and anything that is copyrighted."[34] Anyone who violates the DMCA can be forced to take down or delete copyrighted material from his site.[35] Once the material is taken down, the infringing party will be protected from copyright infringement liability if it qualifies as an online service provider (OSP). The protection derives from a safe harbor clause within the statute which acts as a shield against monetary liability for claims of copyright infringement.[36] Congress determined this protection for OSPs was needed to help usher in the new digital era and to allow technological innovation to flourish.[37] This makes sense as it would hardly be fair to expect Barnes and Noble to bear responsibility for every copyright violation in the multitude of books it displays and sells. Instead, when an author notifies the company of a violation, the book can be removed from the shelf. This same logic applies in the online arena.

Section 512 of the DMCA contemplates four distinct types of OSPs, each of which has different requirements to qualify for safe harbor:

> a) mere conduit (*i.e.,* serving as a conduit for the automatic online transmission of material without modification of its content, as directed by third parties (e.g., cable, DSL or cellular network providers);

---

[31] U.S. Copyright Office, *The Digital Millennium Copyright Act*, COPYRIGHT.GOV, https://www.copyright.gov/dmca/ (last visited June 27, 2025).
[32] Copyright Act, 17 U.S.C. § 106 (1976).
[33] *The Digital Millennium Copyright Act of 1998-S. 2037-105th Congress, CONGRESS.*GOV, https://www.congress.gov/bill/105th-congress/senate-bill/2037 (last visited June 17, 2025).
[34] *Digital Millennium Copyright Act*, WILKES UNIVERSITY, https://www.wilkes.edu/about-wilkes/policies-and-procedures/copyright.aspx (last visited June 17, 2025).
[35] Will Roszcyk, *What is DMCA? The Digital Millennium Copyright Act Explained* (Oct. 5, 2022), ITPRO, https://www.itpro.com/development/web-development/368194/what-is-dmca-the-digital-millennium-copyright-act-explained.
[36] U.S. Copyright Office, *Section 512 of Title 17: Resources on Online Service Provider Safe Harbors and Notice-and-Takedown System*, COPYRIGHT.GOV, https://www.copyright.gov/512/ (last visited June 17, 2025).
[37] Kevin J. Hickey, *Copyright Law: An Introduction and Issues for Congress*, CONGRESS.GOV (Mar. 7, 2023), https://www.congress.gov/crs-product/IF12339.

b) caching (*i.e.,* temporarily storing material that is being transmitted automatically over the internet from one-third party to another (e.g., making a local copy of a website and serving it up to its users who request the original website);
c) storing (*i.e.,* hosting) material at the direction of a user on a service provider's system or network (e.g., websites that host user-generated content); and
d) linking (*i.e.*, referring or linking users to online sites using information location tools (e.g., search engines).[38]

V. DMCA SAFE HARBOR PROTECTION

If anyone engages in any of the four activities listed above, or a combination of them, they will be considered an OSP eligible for a DMCA safe harbor concerning these activities if they comply with the other requirements of section 512. Course Hero seems to fall squarely in the storing/hosting category of 512(c) because it is a website that hosts user-generated content. The next inquiry is whether Course Hero meets the requirements for safe harbor. Those requirements are as follows:

> (1) adopt and reasonably implement a policy to terminate repeat infringers (including users who have repeatedly had material taken down either under the notice-and-takedown process or as the result of the OSP's own "red flag" knowledge of infringing activity, not necessarily as a result of having been found infringing in court);
> (2) accommodate and not interfere with *standard technical measures* [such as copyright symbols and watermarks] that identify or protect copyrighted works that have been developed according to broad consensus between copyright owners and OSPs to the extent any such measures exist.[39]

Course Hero has a policy entitled Notice and Take Down Procedures for Claims of Infringement, which states that Course Hero reserves the right "to terminate accounts of repeated alleged infringers."[40] While the verbiage tracks section 512(c)(1) of the statute, what about the implementation of the policy? How does Course Hero terminate alleged repeat infringers so that it can keep its safe harbor protections? Does Course Hero have a duty to scour its website to seek out alleged infringers? According to the DMCA, the answer is: No. It is the responsibility of the professor (or anyone alleging infringement) to do the scouring and to subsequently notify Course Hero of possible infringement.[41] As stated previously, uploaded work is initially presented in small print or blurred segments necessitating a paid subscription to view the full documents. There is a certain irony in having to contribute to the coffers of the platform profiting from one's work to locate that work. To this point, Alexander Toftness explains in his article that "[i]t certainly appears that Course Hero intentionally makes their website design frustrating and hard to access for people who want to take down their illegally shared materials."[42] Likewise, Wikipedia states

---

[38] 2020 U.S. REGISTRAR OF COPYRIGHTS REP. 23.
[39] 2020 U.S. REGISTRAR OF COPYRIGHTS REP. 24.
[40] *Service Terms for Course Hero -- Notice and Take Down Procedure for Claims of Infringement*. COURSE HERO, (Aug. 29, 2024) https://www.coursehero.co.m/copyright/#/terms-of-use.
[41] Kevin J. Hickey, *Digital millennium Copyright Act (DMCA) Safe Harbor Provisions for Online Service Providers: A Legal Overview*, CONGRESS.GOV (Mar. 30, 2020), https://www.congress.gov/crs-product/IF11478.
[42] Alexander R. Toftness., *How to Take Down Copyrighted Course Materials From Websites Like Course Hero: An unofficial guide for university instructors and TAs (2020),*

under the heading "Copyright Concerns" that "the process to remove copyright material [on Course Hero] is burdensome and discourages people from following through on such claims."[43] Professors should note that the takedown notice to Course Hero must follow the procedure outlined in the U.S. Copyright Office instructions.[44] This is simple enough to do, but only Course Hero can determine if an infringer is a *repeat* infringer that must be terminated in accordance with the statute. A professor is unable to make that determination because names rarely appear on uploaded material. In addition, many users keep their identities concealed behind an obscure username (*i.e.,* donut1), that bears no resemblance to their true names. Without names, it becomes all but impossible for anyone but Course Hero to discern if *repeated* infringements are occurring. Professors (and anyone else suspecting infringement) are blind as to whether it is one student *repeatedly* doing the infringing or *several different* students who are causing *singular* infringement incidents. This is a classic case of the fox guarding the henhouse. A claimant knows that a website is sponsoring cheating with infringed material but must rely on the website enabling cheating to ethically determine if infringement is being repeated which would trigger termination under the statute. This creates a Catch-22 situation for the professor. Unless there is accurate verification of the uploader, infringement can be repeated without repercussion while Course Hero reaps the monetary rewards.

One professor/attorney decided to use the power of the subpoena to navigate around Course Hero's cat-and-mouse game which prevented him from obtaining the name of the student who posted his online exam without his permission. Professor David Berkovitz, a business professor at Chapman University, discovered that a student had posted his final exam on Course Hero. He was disturbed by the unfair effect that cheating on his exam had on his non-cheating students. As Dr. Berkovitz stated, "They did nothing wrong. They studied hard, they didn't cheat, and yet their grade is artificially lower than it should have been because of the curve."[45] According to Dr. Berkovitz during a personal interview conducted by the authors of this paper, Course Hero was far from helpful and tried to thwart him at every turn. He initially tried to resolve the matter by calling an upper-level management employee of Course Hero expecting that person to share his concern that the Course Hero site was being utilized to cheat. Rather than being cooperative Course Hero informed Dr. Berkovitz that a subpoena duces tecum (a subpoena for documents rather than persons) would be necessary before Course Hero would comply. This meant that Dr. Berkovitz would have to file a lawsuit to gain subpoena power.[46]

Rather than sue Course Hero, Dr. Berkovitz sued his students "Doe's 1-5" and issued a subpoena accordingly. This brilliant legal move of suing his nameless students and not Course Hero meant that DMCA defenses were not available to Course Hero.[47] Although Course Hero told *The New York Times* that the company would comply with the court's subpoena in the

---

https://static1.squarespace.com/static/5a1b43e5f43b5510c0ec719d/t/5f3ea2d4a8f40576bd9f51a8/1597940436206/How+to+take+down+copyrighted+course+files+from+Course+Hero+8-17-20+by+Alexander+Toftness.pdf.

[43] *Course Hero*, WIKIPEDIA (Apr. 20, 2025), https://en.wikipedia.org/wiki/Course_Hero.

[44] *Id. See also Copyright Policy*, LEARNEO, https://www.coursehero.com/copyright/#/ (last visited July 16, 2025). Melissa says to use Melaney's link. What is it????

[45] Michael Levenson, *Hoping to Identify Cheaters, a Professor Sues His Own Students*, THE NEW YORK TIMES (Mar. 18, 2022), https://www.nytimes.com/2022/03/17/us/chapman-law-cheating-professor.html.

[46] *How to Subpoena a Witness or Documents*, TEXASLAWHELP.ORG (Mar. 8, 2023), https://texaslawhelp.org/article/how-to-subpoena-a-witness-or-documents.

[47] Colleen Flaherty, *Suing Students Who Shared Exams Online to Identify Them*, INSIDE HIGHER ED (March 18, 2022), https://www.insidehighered.com/news/2022/03/18/suing-students-who-shared-exams-online-identify-them.

Berkovitz case,[48] it is noteworthy that Course Hero filed a thirty-eight-page response to the subpoena raising eight general objections and forty specific objections to it.[49] Perhaps the defendant should have said it would *grudgingly* "comply" kicking and screaming all the way. It is interesting to note that the Berkovitz subpoena requested not only the *identity* of the person(s) who posted an answer to a question from his exam but also a complete history of *when* any such identified person accessed any of the questions and/or answers on any Course Hero Website.[50] This is due to Dr. Berkovitz's suspicion that students taking his online exam were utilizing tutors from Course Hero to answer exam questions in *real time during the exam*.[51] This was a belief bolstered by Course Hero's website which tells students they can "[g]et connected with a verified expert tutor 24/7 and [r]eceive answers and explanations in as few as 30 minutes."[52] The case ultimately did not have to proceed forward as the pressure of the lawsuit caused the student perpetrator to confess to the wrongdoing.[53] This will likely go down as one of the greatest moves in academe folklore of the current century. Kudos to Dr. Berkovitz from professors across this nation as it is now clear where the loyalties of Course Hero truly lie.

VI. RED FLAGS

Another noteworthy gem that was gleaned from the conversation with Dr. Berkovitz was his statement that following the publication of his experience in several media sources, he was contacted by numerous professors from around the country. Professors were disturbed by the fact that despite their work having clear copyright symbols, it nonetheless was posted on the Course Hero website.[54] This puts Course Hero in troubled waters as Section 512 of the DMCA stipulates that Course Hero is not only required to remove material after receiving a takedown notice, but also in those circumstances in which its own "red flag" knowledge of infringing activity is triggered. In the legislative history of the DMCA, Congress considered "red flags" to be those things that cause an OSP to be "aware of facts or circumstances from which infringing activity is apparent, which creates an obligation of expeditious removal."[55] It is hard to imagine a brighter red flag than a copyright symbol to signal that material posted is copyright protected requiring the need to verify if the uploader is the owner, and if she is not, then an immediate takedown of the material must occur. Red flags are dangerous for Course Hero because although it is not statutorily required to monitor its websites for copyright infringement, it cannot willfully blind itself to it.[56]

Willful blindness occurs when an OSP consciously avoids learning about specific instances of infringement.[57] Emphasis on the word *consciously*. Given the number of exams on the Course Hero website, some of which clearly display copyright symbols, it is no stretch of the imagination

---

[48] Michael Levenson, *Hoping to Identify Cheaters, a Professor Sues His Own Students*, THE NEW YORK TIMES (March 18, 2022), https://www.nytimes.com/2022/03/17/us/chapman-law-cheating-professor.html.
[49] Telephone Interview with David A. Berkovitz (2023).
[50] *Id.*
[51] *Id.*
[52] *Homework Help - Q&A From Online Tutor*s, COURSE HERO, https://www.coursehero.com/tutors/homework-help/ (last visited Feb. 5, 2025).
[53] Telephone Interview with David A. Berkovitz (2023).
[54] *Id.*
[55] Nicolo Zingales, *Red Flag Knowledge*, GLOSSARY OF PLATFORM LAW AND POLICY TERMS (Dec. 17, 2021), https://platformglossary.info/red-flag-knowledge/.
[56] *Viacom Int'l, Inc. v. YouTube, Inc.* 676 F.3d 19, 35 (2d Cir. 2012).
[57] 2020 U.S. REGISTRAR OF COPYRIGHTS REP. 124.

to presume that copyright infringement could be afoot. Even without the copyright symbols, it is universally known that professors do not normally desire to share the contents of their exams with current or future students. Therefore, the very word "exam" on the document should trigger a red flag for Course Hero. Willful blindness can be compared to a person plugging her ears to avoid hearing what is being said, or, in the case of Course Hero, seeing what is blatantly posted on its website. Course Hero's days of safe harbor protection under Section 512 of the DMCA may be numbered if it continues to willfully blind itself to the flagrant red flags on its site and continues to use a Terms of Use statement that pays mere lip service to the statutory requirements for safe harbor protection.

VII. FAIR USE

If Course Hero loses its safe harbor protection under the DMCA, its only recourse will be to claim the defense of Fair Use which allows the use of a limited amount of copyrighted material under certain circumstances without getting permission or paying any fees.[58] The courts will examine four factors to determine what qualifies as Fair Use.[59]

First, what is the purpose of the use of the material in question?[60] If the purpose is commercial use rather than educational, it weighs against the defense of Fair Use. Course Hero's subscription service alone brings in a revenue of one hundred million dollars per month.[61] For obvious reasons, Course Hero might be on shaky ground here.

Second, what is the nature of the copyrighted work?[62] Factual works are more likely to be considered Fair Use than highly creative works such as poems and music. An argument can be made that when a professor's work is created using his imagination and intellect tailored for his specific course rather than relying on a test bank or other canned resource for material, it is "creative." Encouraging creative expression is at the core of copyright protection, and this could weigh against the Fair Use defense for Course Hero in the right circumstances.[63]

Third, how much of the copyrighted work was used?[64] While there is no magic formula that courts apply for the quantity used, since Course Hero uses the entirety of each piece of work product posted, it could prove problematic for Course Hero in the eyes of the court.

Fourth, how much of the copyrighted work's market value is affected by Course Hero's use of it?[65] It is unknown how this will be viewed by a court in the academic realm, but here are

---

[58] *Fair Use,* GEORGETOWN UNIVERSITY LIBRARY. https://library.georgetown.edu/copyright/fair-use (last visited June 18, 2025).
[59] Richard Stim & Glen Secor, Fair Use: The 4 factors Courts Consider in a Copyright Infringement Case, NOLO (updated June 20, 2023), https://www.nolo.com/legal-encyclopedia/fair-use-the-four-factors.html.
[60] *Id.*
[61] Alexander R. Toftness, *How to Take Down Copyrighted Course Materials From Websites Like Course Hero: An unofficial guide for university instructors and TAs (2020)*, https://static1.squarespace.com/static/5a1b43e5f43b5510c0ec719d/t/5f3ea2d4a8f40576bd9f51a8/1597940436206/How+to+take+down+copyrighted+course+files+from+Course+Hero+8-17-20+by+Alexander+Toftness.pdf.
[62] Richard Stim & Glen Secor, Fiar Use: The 4 factors Courts Consider in a Copyright Infringment Case, NOLO (updated June 20, 2023), https://www.nolo.com/legal-encyclopedia/fair-use-the-four-factors.html.
[63] Copyright Information – Fair Use, PENNSTATE, https://copyright.psu.edu/copyright-basics/fair-use (last visited June 18, 2025).
[64] Richard Stim & Glen Secor, Fiar Use: The 4 factors Courts Consider in a Copyright Infringment Case, NOLO (updated June 20, 2023), https://www.nolo.com/legal-encyclopedia/fair-use-the-four-factors.html.
[65] *Id.*

a few facts to digest. As this paper is being read, a multitude of students are busily uploading exams, quizzes, discussion boards, and other assignments to Course Hero which are the work product of university professors across all fifty states. In 2021, Course Hero was listed as having two million annual subscribers on its platform with plans to reach fifty million by 2030.[66] There is currently an endless flow of copyrighted material on the Course Hero site, much of which is being utilized to cheat. Every academic institution across the United States is affected when their Honor Codes are violated in this manner. Just as the court in the infamous Napster case involving music downloads found that Napster's online operation went against public policy because the "market effect" on the music industry was significant, the same should hold true for the educational industry.[67] Every time students cheat, it waters down the value of their degrees and presents an ethical calamity for every company that unwittingly hires those students who have cheated their way to the job. The purpose of Honor Codes at a university is to ensure a level playing field for all students and to prepare them for future employment and ethical contributions to society. They allow the best and the brightest and those with a strong work ethic to rise to the top. Course Hero's business model defeats this purpose. However, the bell may be tolling for Course Hero as a barrage of copyright infringement lawsuits could be forthcoming.

VIII. ONLINE PROCTORING

Course Hero and similar websites are not the only problems that universities fighting for academic integrity are facing. Online education is creating some difficulties as well. More than ten million college students are enrolled in online classes at public higher education institutions.[68] Add a pandemic to the mix, and academic dishonesty reports at Texas A&M and the University of North Texas increased by as much as twenty percent. Texas State University also saw reports of cheating increase by one-third over the previous fall.[69] The common denominator was more classes being delivered online, which created academe's second foe: students attempting to circumvent online proctoring.

Exam proctoring has been in existence since the scribes of ancient civilizations were employed to write exam questions and monitor students while they took their exams.[70] Classrooms across America have long followed this practice, with teachers or professors walking around the room to observe students while they take an exam ensuring no one succumbs to the temptation to cheat. Proctoring exams is a hallmark of academic integrity that must be preserved whether one is taking an exam in person or online. The need for online proctoring has been met by several online proctoring services which differ somewhat in how they deliver their product. Some use a live proctor, such as ProctorU, while others, such as Honorlock, use Artificial Intelligence (AI) to monitor student behavior during an exam. A human proctor is alerted if AI detects potential

---

[66] Vikant Chaturvedi. *Course Hero Hits $3.6B Valuation For Its Online Class Study Materials Technology. Competitors Include Studypool, Chegg, StuDocu, And Quizle*, CBINSIGHTS (Dec. 16, 2021). https://www.cbinsights.com/research/course-hero-series-c-funding/.

[67] *A&M Records, Inc. v. Napster, Inc.,*239 F.3d 1004, 1018 (9th Cir. 2001).

[68] Ilana Hamilton, *2024 Online Learning Statistics*, FORBES (June 3, 2024), https://www.forbes.com/advisor/education/online-learning-stats/.

[69] Kate McGee, *Texas A&M Investigating 'Large Scale' Cheating Case as Universities See More Academic Misconduct in ERA of Online Classes,* THE TEXAS TRIBUNE (Dec. 16, 2020), https://www.texastribune.org/2020/12/16/texas-am-chegg-cheating/.

[70]*What Is the History of Exam Proctoring?*, PROCTORFREE (Jan. 9, 2023), https://www.proctorfree.com/news/what-is-the-history-of-exam-proctoring.

cheating. Unfortunately for ProctorU, there is a website devoted solely to methods to defeat ProctorU's anti-cheating mechanisms. The website contains the following language: "You might have forgotten to prepare for the tests and exams due to functions at your house. Don't panic; dive deep into the article to learn how to cheat in online exams despite ProcterU supervision."[71] To add fuel to the fire, an organization called Fight for the Future is gathering signatures to ban E-proctoring.[72] Students are on the warpath and seem to be willing to do anything to defeat online proctoring. A good case in point is the story of Aaron Ogletree.

IX. THE OGLETREE CASE

Aaron Ogletree was a student at Cleveland State University (CSU) who filed a lawsuit against CSU for the scan of his room before his online exam. Mr. Ogletree claimed the scan was a violation of his Fourth Amendment right against unreasonable searches and seizures. CSU disagreed, and the battle was on in the Federal District Court in the Northern District of Ohio.[73] In a surprising decision rendered on August 22, 2022, the court ruled in favor of Aaron Ogletree. To understand the decision, a brief look at Fourth Amendment jurisprudence and the specific facts of the case is necessary. The Fourth Amendment to the United States Constitution protects "[t]he right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures."[74] The Fourth Amendment protects against governmental intrusions and, therefore, applies to searches of public-school students by public-school officials.[75] Since public universities receive federal funding, they are considered to be an arm of the government. Therefore, students are entitled to the protections of the U.S. Constitution. Consequently, Aaron Ogletree and every other student at a public university has the right to be free from unreasonable searches and seizures perpetrated upon them by their university. The pivotal questions to be addressed are: Is a room scan a search, and if so, is it unreasonable?

> An examination of the facts outlined by the District Court reveals the following:
> [A]t 10:25 am almost *two hours before scheduled exam* [emphasis added], Cleveland State Testing Services emailed Mr. Ogletree to inform him that the Proctor would be "checking [his] ID, [his] surroundings, and [his] materials." (citation omitted) At 10:40 am, Mr. Ogletree replied to the email. (citation omitted) Mr. Ogletree explained that he "currently [had] confidential settlement documents in the form of late arriving 1099s scattered about [his] work area and there [was] not enough time to secure them. (citation omitted)
> At the start of the exam, the proctor asked Mr. Ogletree to perform a room scan of his bedroom, and *Mr. Ogletree complied* [emphasis added]. (citation omitted) The

---

[71] George Orwell, *ProctorU Cheating Guide for College Students*, STUDENTS ASSIGNMENT HELP (Nov. 9, 2021), https://www.studentsassignmenthelp.com/blogs/proctoru-cheating-guide/.
[72] *Tell McGraw-Hill that Proctorio proctoring software is …,* FIGHT FOR THE FUTURE (Feb. 10, 2021), https://www.baneproctoring.com/.
[73] Ogletree v. Cleveland State University*,* 647 F. Supp. 3d 602 (N.D. Ohio 2022). The Sixth Circuit granted a consolidated motion for vacatur and dismissed the appeal as moot due to the death of Amelia Ogletree (nee Aaron M. Ogletree). It remanded the case to the district court and instructed the court to vacate its judgment and dismiss the complaint. (Laura Bloomberg was the President of Cleveland State University.) Ogletree v. Bloomberg, 2023 WL 8468654 (6th Cir., Dec. 4, 2023).
[74] U.S. CONST. amend. IV.
[75] New Jersey v. T.L.O., 469 U.S. 325, 341-42 (1985).

> scan lasted less than a minute, and as little as ten to twenty seconds. (citation omitted) [Mr. Ogletree had control of the scan of the room and which areas would be viewed.] The proctor testified that she did not see any tax documents or medications. (citation omitted)
> The room scan and the test were recorded, and the video recording was retained by Cleveland State's third-party vendor. (citation omitted) Cleveland State [was] not aware of any data breaches related to remote exam recordings, and access to the video [was] strictly controlled. (citation omitted)[76]

A search can occur in one of two ways: (1) by a physical intrusion of a person, house, or papers, or (2) the government's violation of a person's subjective expectation of privacy that society recognizes as reasonable.[77] "At the Fourth Amendment's 'very core' lies the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."[78] The court in the *Ogletree* case determined, and most would agree, that a bedroom within one's house deserves an expectation of privacy. Therefore, a search occurred, but the question remains: Was it unreasonable? Fourth Amendment jurisprudence generally would find a search without suspicion of an illegal activity to be unreasonable.[79] However, "an exception exists in certain circumstances where the government has 'special needs beyond the normal need for law enforcement'"[80] "Where a governmental intrusion serves 'special needs,' courts must balance the individual's privacy expectations against the State's interest to assess a search's unreasonableness and the practicality of the warrant and probable-cause requirements in the particular context."[81] In layman's terms, as it applies to the *Ogletree* case, it came down to whether CSU's "special need" for exam integrity outweighed Aaron Ogletree's privacy expectations. The *Ogletree* court found that it did not and decided in favor of Mr. Ogletree. The Ohio District Court quoted the United States Supreme Court's statement about constitutional encroachments when the Court stated, "It may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedure."[82] Some might quibble with whether there were any illegitimate or unconstitutional practices carried out by CSU's brief scan of Aaron Ogletree's room for which he had two hours to prepare. Before academic panic ensues, it should be noted that part of the Ohio court's reasoning included the fact that it was during the COVID pandemic and Mr. Ogletree had no choice but to enroll in an online class. Under normal circumstances, he would have had more options to avoid the scan of his room which he considered intrusive. For instance, he could take classes on campus. Due to Mr. Ogletree's unforeseen death[83], an appellate court will not have the opportunity to weigh the relevance of these factors as well as:

---

[76] Ogletree v. Cleveland St. U., 647 F. Supp. 3d 602, 609 (N.D. Ohio 2022).
[77] Moore Law Firm, PLLC, 2021. *What Is a Search Under the Fourth Amendment?* THE MOORE LAW FIRM, PLLC (May 17, 2021), https://www.moorelawfirmwv.com/blog/2021/.
[78] Florida v. Jardines, 569 U.S. 1, 6 (2013).
[79] Vernonia Sch. District. 47J v. Acton, 515 U.S. 646, 652 (1995).
[80] Griffin v. Wisconsin, 483 U.S. 868, 873 (1987).
[81] Ogletree v. Cleveland St. U., 647 F. Supp. 3d 602, 614 (N.D. Ohio 2022) (citing Skinner v. Railway Lab. Execs.' Ass'n, 489 U.S. 602, 619-20 (1989)).
[82] Silverman v. U.S., 365 U.S. 505, 512 (1961) (quoting Boyd v. United States, 116 U.S. 616, 635 (1886).
[83] *See note* 73.

- the two hours Ogletree had prior to the exam to hide or turn face-down the papers of concern in his room;
- the personal control he had over the room scan and what would be viewed by any onlookers;
- the fact that he complied with the search; and
- the need for universities to maintain the integrity of their exams.

It is not difficult to imagine an appellate court reaching a conclusion that differs from the lower court. Also, it should be remembered that this case is not controlling precedent anywhere outside of its jurisdiction, which is limited to forty of the most northern counties in Ohio.[84]

If proctoring services cannot be utilized, what other methods are there to preserve the integrity of online exam results? Open-book exams with strict time constraints are an option, but this creates a high likelihood that the exam will be compromised through downloading, copying, or photographing the exam for the next round of students. Another alternative is requiring students to take exams at a facility near their residence that offers live proctoring. This alternative is more expensive but would certainly minimize cheating. Unfortunately, one can already imagine the difficulty of enforcing this arrangement as the excuses, legitimate or otherwise, will be rampant. The sounds of "I don't have a way to get there," or "I can't afford the cost," or "I have an accommodation that will not allow me to do it that way" are already wafting through the air. Students might do much better in their classes if they devoted as much time to their studies as they do to complaining about the proctoring systems universities are trying to put in place to defeat cheating. The battle lines have been drawn, and the future of online proctoring remains uncertain.

X. CONCLUSION

There is no doubt that technology has made for some rough terrain for universities fighting for academic integrity. The legal obstacles from online service providers and litigious students determined to cheat have created an uphill battle. However, the battle is worth fighting for as academic integrity is the bedrock of academe. Universities must stand firm, or the future will be bleak. The German philosopher Immanuel Kant espoused a universal law regarding ethical decision-making which can be summarized by asking: What would happen if everyone engaged in the same unethical conduct?[85] In terms of academic integrity, what would happen if every student at a university cheated? The answer is that a degree would be meaningless, and universities would become obsolete. A chilling thought that universities would be wise to remember.

---

[84] *Court Info*, U.S. DISTRICT COURT NORTHERN DISTRICT OF OHIO, https://www.ohnd.uscourts.gov/court-info (last visited May 30, 2025).

[85] Philosophy Terms, *Categorical Imperative*, https://philosophyterms.com/categorical-imperative/ (last visited July 16, 2025).

SECURITIES AND EXCHANGE COMMISSION ADOPTING A BROAD VIEW OF LIABILITY FOR CYBERSECURITY-RELATED DISCLOSURES AND INTERNAL ACCOUNTING CONTROLS UNDER SECURITIES LAWS

RICARDO COLÓN[*]
ÁNGEL ORTIZ[**]

I. INTRODUCTION

Businesses face increased scrutiny vis-a-vis cybersecurity incidents under U.S. securities laws. An area of particular concern is public company disclosures and internal controls. From January 2018 to June 2024, the U.S. Securities and Exchange Commission (SEC) filed at least seven enforcement actions against public companies based on the disclosures of cybersecurity-related incidents or internal control deficiencies. Some SEC enforcement actions have garnered substantial attention owing to the agency's expansive interpretation of securities laws to impose liability on companies that have been the target of cybersecurity incidents. Although cybersecurity incidents seem ubiquitous in today's business environment, public companies have legal obligations under securities laws for cybersecurity-related internal controls and disclosures.

This paper analyzes the longstanding securities laws, new regulations, and recent SEC guidance that sets forth the obligations of public companies with respect to cybersecurity. Subsequently, it discusses seven enforcement actions filed by the SEC against companies that have violated the securities laws concerning cybersecurity-related disclosures or internal accounting controls. Finally, it concludes that companies face increasing liability under the SEC's broad interpretation of securities laws and new rules related to cybersecurity.

II. SECURITIES LAWS, RULES AND ADMINISTRATIVE GUIDANCE RELATED TO CYBERSECURITY

Although cybersecurity incidents that threaten a public company's assets may be a recent occurrence, the expectation that public companies will have sufficient internal accounting controls that are reviewed and updated as needed is not new.[1] Sections 13(b)(2)(B)(i) and (iii) of the Securities and Exchange Act of 1934 require public companies to devise and maintain a system of internal accounting controls sufficient to provide reasonable assurance that "transactions are executed in accordance with management's general or specific authorization" and that "access to assets is permitted only in accordance with management's general or specific authorization." Similarly, Exchange Act Rule 13a-15(a) requires public companies to maintain disclosure controls

[*]LL.M., J.D., Associate Professor of Accounting, Lamar University.
[**] DBA, J.D., MBA, Associate Professor of Accounting, University of Puerto Rico at Cayey.
[1] Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements, Release No. 84429 (Oct. 16, 2018), https://www.sec.gov/files/litigation/investreport/34-84429.pdf

and procedures designed to ensure that the information required to be disclosed by a public company is recorded, processed, summarized, and reported within the period specified in the SEC's rules and forms.

Moreover, Securities Act Rule 408, Exchange Act Rule 12b-20, and Exchange Act Rule 14a-9 implicitly require the disclosure of material information regarding cybersecurity risks and cyber incidents when necessary to make other required disclosures, based on the circumstances in which they are made, not misleading. Additionally, public companies are required to disclose cyber incidents' risk if such events are among the most significant factors that render investment in the company speculative or risky.[2] Generally, cybersecurity risk disclosures must adequately describe the material risks' nature and specify how each risk affects the public company.[3] Public companies should address cybersecurity risks and cyber incidents in their Management Discussion and Analysis of Financial Condition and Results of Operations (MD&A) if such risks are material to the financial statements.[4] Finally, public companies should consider the antifraud provisions of the federal securities laws, which apply to statements and omissions both inside and outside SEC filings.[5]

In 2011, the SEC Division of Corporate Finance issued guidance covering disclosure obligations regarding cybersecurity risks and incidents. This guidance called for public companies to consider the following disclosures: (1) aspects of the business or operations that precipitate material cybersecurity risks and the potential costs and consequences; (2) the extent to which the company outsources functions that have material cybersecurity risks, a description of those functions and how the company addresses those risks; (3) the occurrence of cyber incidents that are individually, or in the aggregate, material, including a description of the costs and other consequences; (4) risks related to cyber incidents that may remain undetected for an extended period; and (5) a description of the relevant insurance coverage.[6]

Subsequently, in 2018, the SEC issued an Interpretive Release elucidating how existing disclosure rules apply to cybersecurity risks and incidents and calling for public companies to adopt "all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack."[7]

Although disclosures of cybersecurity-related risks and incidents improved after the guidance issued by the Division of Corporate Finance and the Interpretive Release, disclosure practices remained inconsistent.[8] Consequently, in 2023, the SEC adopted new rules to "enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incidents by public companies that are subject to the reporting requirements of the Securities

[2] *See* Item 503(c) of Regulation S-K; and Form 20-F, Item 3.D.
[3] *See* Item 503(c) of Regulation S-K.
[4] *See* Item 503(c) of Regulation S-K; and Form 20-F, Item 4.B.
[5] *See* Securities Act Section 17(a); Exchange Act Section 10(b); and Exchange Act Rule 10b-5.
[6] CF Disclosure Guidance: Topic No. 2 – Cybersecurity (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm
[7] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release No. 33-10459 (Feb. 21, 2018) [83 FR 8166 (Feb. 26, 2018)], available at https://www.sec.gov/rules/interp/2018/33-10459.pdf
[8] Erik Gerding, Director, Division of Corporation Finance, Statement: Cybersecurity Disclosure (Dec. 14, 2023) [hereinafter *Gerding Statement*].

Exchange Act of 1934."[9] The following table summarizes the new requirements adopted in the new rules issued by the SEC.[10]

Item	Summary Description of the new Disclosure Requirement
Regulation S-K Item 106(b) – *Risk Management and strategy*	Public companies must describe their process, if any, for the assessment, identification, and management of material risks from cybersecurity threats, and describe whether any risks from cybersecurity threats have materially affected—or are reasonably likely to materially affect—their business strategy, results of operations, or financial condition.
Regulation S-K Item 106(c) – *Governance*	Public companies must: 1. describe the board's oversight of risks from cybersecurity threats; and 2. describe management's role in assessing and managing material risks from cybersecurity threats.
Form 8-K Item 1.05 – *Material Cybersecurity Incidents*	Public companies must disclose any cybersecurity incident that they experience that is determined to be material and describe the material aspects of its: (1) nature, scope, and timing; and (2) impact or reasonably likely impact. An Item 1.05 Form 8-K must be filed within *four* business days of determining an incident was material. A public company may delay filing if the United States Attorney General determines immediate disclosure would substantially threaten national security or public safety. Public companies must amend a prior Item 1.05 Form 8-K to disclose any information called for in Item 1.05(a) that was not determined or was unavailable at the time of the initial Form 8-K filing.
Form 20-F	Foreign Private Issuers (FPIs) must: (1) describe the board's oversight of risks from cybersecurity threats; and (2) describe management's role in assessing and managing material risks from cybersecurity threats.
Form 6-K	On Form 6-K, FPIs must furnish information regarding material cybersecurity incidents that they disclose or otherwise publicize

[9] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release Nos. 33-11216; 34-97989 (July 26, 2023), https://www.sec.gov/files/rules/final/2023/33-11216.pdf

[10] *Id.* (Table adapted from Final Rule). *See also* Fact Sheet: Public Company Cybersecurity Disclosures; Final Rules (2023), https://www.sec.gov/files/33-11216-fact-sheet.pdf

	in a foreign jurisdiction, to any stock exchange, or to security holders.
Inline XBRL	The final rules require the cybersecurity disclosures to be presented in Inline eXtensible Business Reporting Language ("Inline XBRL").

Importantly, the new rules do not prescribe specific cybersecurity defenses, practices, technologies, risk management, governance, or strategies.[11] Therefore, public companies have the flexibility to decide how to address cybersecurity risks and threats based on their facts and circumstances.[12]

III. SEC ENFORCEMENT ACTIONS

Despite the issuance of interpretations and disclosure guidance related to cybersecurity and internal controls, the SEC filed seven enforcement actions related to cybersecurity disclosures and internal control matters related to public companies from January 2018 to June 2024. Understanding these cases is essential to explore the specific securities laws and regulations violated by public companies and enhance internal controls and disclosures regarding cybersecurity.

A. Administrative Enforcement Actions

1. Altaba, Inc. (formerly known as Yahoo! Inc.)

Yahoo, a publicly traded internet media company, experienced a data breach over a few days in December 2014.[13] After the breach, Yahoo's information security team discovered that Russian hackers had stolen what they internally referred to as the company's "crown jewels", that is, their clients' database. This information included email addresses, usernames, birthdates, phone numbers, encrypted passwords, and security questions and answers for over 500 million user accounts. Despite reports to senior management and the legal department, Yahoo failed to thoroughly investigate the breach and neglected to consider whether it needed to be disclosed to investors. The breach was not made public until more than two years later, in 2016, during the closing of Yahoo's acquisition by Verizon Communications, Inc.

Yahoo failed to reveal the theft of its users' personal data in its public filings. Instead, the risk factor disclosures in its annual reports for the years ending on December 31, 2014 and December 31, 2015, as well as its quarterly reports for the first three quarters of 2015 and the first two quarters of 2016, mistakenly implied that a significant data breach had not occurred. Consequently, the filings only suggested in boilerplate language that the company faced a risk of data breaches and any potential negative impacts that might arise from future breaches. Furthermore, Yahoo's filings failed to discuss the breach's potential effect on the company's

[11] *Gerding Statement, supra* note 8, at 3.
[12] *Id.*
[13] *In re Altaba Inc.*, Admin. Proc. No. 3-18448 (Apr. 24, 2018), https://www.sec.gov/files/litigation/admin/2018/33-10485.pdf

business in its risk factors; moreover, they did not report the known trends or uncertainties regarding liquidity or net revenue related to any current or future expenses and losses linked to the 2014 data breach in their annual report's MD&A section.

Yahoo violated Sections 17(a)(2) and 17(a)(3) of the Securities Act and Section 13(a) of the Exchange Act. First, the company violated Sections 17(a)(2) and 17(a)(3) of the Securities Act because it engaged in a transaction to offer or sell securities with misleading information to defraud or deceive a purchaser. Specifically, Yahoo offered to sell securities to Verizon without notifying the purchaser or previously disclosing the data breach incidents to the SEC. Second, Yahoo violated Section 13(a) of the Exchange Act and Rules 12b-20, 13a-1, 13a-11, 13a-13, and 13a-15 thereunder because it did not timely file and disclose data breach incidents in its quarterly and annual reports. The company did not have in place disclosure controls or procedures designed to ensure that data security incidents and information were reported within the period specified in the SEC's rules and forms. The SEC imposed a civil sanction of $35,000,000 in a settlement, without Yahoo accepting or denying the SEC's allegations.

2. First American Financial Corp.

First American Financial Corp., a public company that provides products and services related to commercial and residential real estate transactions, experienced a data breach in its system, which was identified and notified by a journalist.[14] On May 24, 2019, a cybersecurity journalist made First American aware of a vulnerability in its application, which had exposed over 800 million title and escrow document images dating back to 2003. These images included sensitive personal data such as social security numbers and financial information. Subsequently, First American issued a statement to be included in the journalist's report, which was published on the evening of May 24, 2019, and provided a Form 8-K to the SEC on May 28, 2019. However, senior executives at First American responsible for the press statement and Form 8-K were not provided with certain crucial information. First, the company's information security personnel had prior knowledge regarding the vulnerability associated with their system, namely, EaglePro, which was essential for the management's evaluation of the company's response to the vulnerability and associated risks. Second, the company's executives were not aware that information security personnel had identified a vulnerability several months earlier in a manual penetration test of the EaglePro application (referred to as the "January 2019 Report"), or that the company had failed to address the vulnerability in line with its policies. First American's disclosure controls and procedures could not provide pertinent information to senior management before the company disclosed the vulnerability.

Based on the SEC's investigation, senior executives responsible for the company's May 2019 statements failed to assess whether they should disclose the company's prior knowledge of—or actions related to—the vulnerability. As these senior executives were unaware of the January 2019 report, they were also unaware of the vulnerability described therein. Unbeknown to them, the company's information security team knew about the vulnerability for months, but the information technology team did not address it, leaving millions of document images exposed to potential unauthorized access. Furthermore, after Form 8K was submitted, the company's information security team determined that the vulnerability had been present since 2014. Consequently, senior executives lacked crucial information to fully assess the company's

[14] *In re First Am. Fin. Corp*., Admin. Proc. No. 3-20367 (June 14, 2021), https://www.sec.gov/files/litigation/admin/2021/34-92176.pdf

cybersecurity responsiveness and the extent of the risk posed by the system's vulnerability when approving the company's disclosures.

First American violated Rule 13(a)-15(a) of the Exchange Act. The violation comprised a lack of disclosure controls and procedures designed such that senior executives could timely learn about and report cybersecurity risks and incidents to the SEC. First American reached a settlement with the SEC for a civil penalty of $487,616, without accepting or denying the allegations.

3. Pearson plc

Pearson plc, a London-based public company that provides educational and publishing services, experienced a data privacy and confidentiality breach related to school and university student data.[15] Pearson misrepresented facts and failed to disclose information regarding the 2018 data breach, which compromised the personal information and login credentials of 13,000 educational institution customers. In its Form 6-K report filed in July 2019, Pearson inaccurately referenced a data privacy incident as a potential risk using boilerplate language, despite the known occurrence of the 2018 cyber-attack. Furthermore, in a media statement, Pearson falsely suggested that the breach might have involved birth dates and email addresses, knowing that such data had indeed been stolen. Moreover, the media statement omitted to disclose the theft of millions of student data records, usernames, and passwords. Pearson claimed to have stringent security measures in place, though it neglected to address a critical vulnerability for six months after being alerted to it.

Pearson violated Sections 17(a)(2) and 17(a)(3) of the Securities Act, Section 13(a) of the Exchange Act, and Rules 12b-20 and 13a-16 thereunder. Initially, the company violated Sections 17(a)(2) and 17(a)(3) of the Securities Act because it offered or engaged in transactions to offer or sell securities with misleading information to defraud or deceive purchasers. Per the investigation, the stock price decreased by 3.3% the day after the Form 6-K report was issued. Moreover, the Form 6-K report was inaccurate and misleading. Under *Aaron v. SEC*, the SEC only had to show the company's negligence and did not have to prove Pearson's scienter or fraudulent intentions to establish a violation of this section.[16] Additionally, Pearson violated Section 13(a) of the Exchange Act and Rules 12b-20, 13a-1, 13a-11, 13a-13, and 13a-15 thereunder because the company did not timely disclose the data privacy and confidentiality breach incident. The company should have maintained disclosure controls and procedures to timely report cybersecurity incidents. Pearson reached a settlement with the SEC of $1,000,000 as a civil penalty, without accepting or denying the allegations.

4. NVIDIA Corp.

NVIDIA produces and markets graphic processing units (GPUs) for computer applications and video games. In 2018, the company experienced an unexpected increase in the use and demand for GPUs in its systems related to crypto-asset transactions (crypto mining), predominantly from China, but did not disclose it.[17] NVIDIA's sales personnel knew that the unexpected increase in

[15] *In re Pearson plc*, Admin. Proc. No. 3-20462 (Aug. 16, 2021), https://www.sec.gov/files/litigation/admin/2021/33-10963.pdf
[16] *Aaron v. SEC*, 446 U.S. 680, 685, 701-02 (1980).
[17] *In re NVIDIA Corp.*, Admin. Proc. No. 3-20844 (May 6, 2022), https://www.sec.gov/files/litigation/admin/2022/33-11060.pdf

GPU use was driven by crypto mining rather than gaming. As such, the company launched a new product line for crypto mining processors in 2018. The company did not report the unexpected use and demand for crypto mining and the new revenue source of crypto mining instead of video game GPUs.

In 2018, NIVIDIA filed two Forms 10-Q reporting substantial growth in its gaming line. However, the company failed to disclose that this significant fluctuation in revenues and earnings was predominantly attributable to crypto mining, a significant factor impacting its gaming sales. This omission deprived investors of relevant information regarding the volatile nature of crypto events, which may be pertinent to investors in making their assertions to predict prior over future performance of the company's revenues. The SEC determined that NVIDIA's failure to disclose material details regarding the expansion of its gaming business was misleading, especially considering that the company's statements regarding other aspects of its operations were influenced by crypto demand. These reports created the impression that the gaming business was not significantly impacted by crypto mining.

NVIDIA violated Sections 17(a)(2) and 17(a)(3) of the Securities Act, Sections 13(a) and 13(b) of the Exchange Act, and Rules 12b-20, 13a-13 and 13a-15 thereunder. Initially, the company violated Sections 17(a)(2) and 17(a)(3) of the Securities Act because it engaged in transactions by offering and selling securities that provided misleading information. Specifically, the company offered and sold securities to its employees as part of employee incentive plans and stock purchase plans, with inaccurate and misleading information for purchasers. The SEC found that the company was negligent in providing inaccurate information. Moreover, NVIDIA violated Section 13(a) of the Exchange Act and Rules 12b-20, 13a-13 and 13a-15 thereunder because it did not disclose the unexpected transactions and demand for GPUs identified by the selling personnel owing to crypto mining and their impact on revenues and earnings. The company should have maintained disclosure controls and procedures to timely report unexpected transactions and their impact on financial statements. NVIDIA reached a settlement with the SEC of $5,500,000 as a civil penalty, without accepting or denying the allegations.

5. Blackbaud, Inc.

Blackbaud is a public company that suffered a ransomware attack that resulted in unauthorized access to its systems and the exfiltration of sensitive customer information in 2020.[18] Blackbaud offers donor relationship management software to a wide range of non-profit organizations, including charities, religious groups, cultural organizations, higher education institutions, schools, and healthcare organizations. Per the SEC's investigation, the company experienced a cyberattack whereby over one million files from approximately 13,000 customers were exposed. The data included donors' social security numbers and bank account information.

Blackbaud initially declared on July 16, 2020, that the ransomware perpetrator did not compromise donor bank account details or social security numbers. However, shortly after this statement, the company's technology and customer relations staff discovered that the perpetrators had indeed accessed and captured this sensitive data. Nevertheless, in August 2020, the company submitted a quarterly report, Form 10-Q, to the SEC, which omitted crucial details regarding the extent of the breach and misleadingly portrayed the risk of the perpetrator acquiring sensitive donor information as mere speculation. In September 2020, Blackbaud filed a Form 8-K revealing

[18] *In re Blackbaud, Inc.*, Admin. Proc. No. 3-21339 (Mar. 9, 2023), https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-48.pdf

that, sensitive donors' data had indeed been accessed. Employees had failed to relay this critical information to the senior management responsible for public disclosures because of the company's inadequate disclosure controls and procedures. During this period, the company offered and sold shares to its employees as part of its incentive compensation plan and reported this to the SEC in Form S-8.

Blackbaud violated Sections 17(a)(2) and 17(a)(3) of the Securities Act, Section 13(a) of the Exchange Act, and Rules 12b-20 and 13a-13 thereunder. First, the company violated Sections 17(a)(2) and 17(a)(3) of the Securities Act because it engaged in transactions by offering and selling securities with misleading information to its employees as part of its employee incentive plan. As such, the company was considered negligent because it provided inaccurate information. Second, Blackbaud violated Section 13(a) of the Exchange Act and Rules 12b-20, and 13a-13 thereunder because the company did not timely disclose the exfiltration of sensitive information identified by technology and customer relations personnel. The company should have maintained disclosure controls and procedures to timely identify and report cybersecurity incidents. Blackbaud reached a $3,000,000 settlement with the SEC as a civil penalty, without accepting or denying the allegations.

6. R.R. Donnelley & Sons Co.

R.R. Donnelley & Sons Co. (RRD) provides business communications and marketing services. In November and December 2021, RRD had a ransomware network attack that ended with computer encryption, data exfiltration, and service disruptions.[19] The company had a third-party managed security services provider (MSSP), which identified a high number of alerts in the network and escalated them to the RRD's internal cybersecurity personnel. Owing to the high volume and complexity of alerts, RRD security personnel failed to prioritize, respond to, and report the incidents. During this period, hackers extracted data from approximately 22,000 clients, which contained personal and financial information. On December 23, 2021, RRD security personnel finally responded to the cyberattack by shutting down the system and notifying clients as well as state and federal agencies. On December 27, 2021, RRD disclosed the incidents in SEC filings.

RRD violated Section 13(b)(2)(B) of the Exchange Act and Rule 13a-15(a) thereunder. First, RRD violated Section 13(b)(2)(B) because it lacked internal accounting controls to limit access to company assets to management or employees with specific authorization. Second, the company violated Rule 13a-15(a) because it lacked disclosure controls to timely report cybersecurity incidents, according to SEC rules. RRD reached a $2,125,000 settlement with the SEC as a civil penalty, without accepting or denying the allegations. This settlement was notable in two ways:

> "1. [i]t departs from the traditional disclosure related theories that have underpinned previous settlements related to cyber incidents; and 2. [i]t extends the internal accounting controls provisions of Section 13(b)(2)(B) of the Exchange Act, which the SEC has already used to resolve other financial reporting and disclosure cases,

[19] *In re R.R. Donnelley & Sons Co.*, Admin. Proc. No. 3-21969 (June 18, 2024), https://www.sec.gov/files/litigation/admin/2024/34-100365.pdf

to a company's IT systems, as well as related policies and procedures relating to cybersecurity."[20]

B. Court Action

1. Complaint *SEC v. SolarWinds, Corp. & Brown*

In 2023, the SEC filed a complaint in the Southern District of New York stating that SolarWinds Corp. and Timothy Brown—the company's Chief Information Security Officer (CISO)—identified multiple cybersecurity risks and vulnerabilities without disclosing them, defrauding investors in an Initial Public Offering (IPO).[21] The SEC alleged that SolarWinds and its CISO knew about the company's poor cybersecurity practices and substantial vulnerabilities since 2018. However, the company's IPO registration statement dated October 2018 disclosed only generic and hypothetical cybersecurity risks, presenting customers and investors with a different picture of their internal discussions, assessments, and risks regarding vulnerabilities and cyberattacks.

Later, in 2020, the "SUNBURST" attack occurred on the company's software, whereby perpetrators had coding and access to over 18,000 customer systems worldwide. Several customers experienced cyberattacks and notified SolarWinds. On December 14, 2020, SolarWinds filed Form 8-K with the SEC, disclosing that its network had malicious code inserted by the perpetrators in a supply chain attack. However, the SEC concluded that the disclosure was misleading because the company had prior knowledge of this incident, and several customers had experienced—and informed about—cyberattacks over a six-month period. After filing Form 8-K, the stock price dropped by 16% in one day and continued dropping by approximately 35% in a month.

According to the complaint, SolarWinds and its CISO violated Sections 17(a)(2) and 17(a)(3) of the Securities Act; Section 10(b)-5(b) and Rule 10b-5 thereunder; and Sections 13(a) and 13(b) of the Exchange Act, and Rules 12b-20, 12b-20, 13a-1, 13a-11, 13a-13 and 13a-15 thereunder. First, the SEC alleged that SolarWinds and its CISO (aiding the company) violated Sections 17(a)(2) and 17(a)(3) of the Securities Act because they engaged in transactions to offer and sell securities providing misleading information to IPO purchasers. Second, SolarWinds and its CISO violated Section 10(b)-5(b) and Rule 10b-5 because both, with scienter, employed "devices, schemes, or artifices" to defraud investors in purchasing company's securities.[22] The SEC alleged that they engaged in acts to defraud purchasers by knowingly providing false information including information on their website. SolarWinds and its CISO knew about cybersecurity vulnerabilities and risks for numerous years but disclosed a different picture in their SEC reports and website. Third, SolarWinds—aided by its CISO—violated Sections 13(a) and 13(b) of the Exchange Act, and Rules 12b-20, 12b-20, 13a-1, 13a-11, 13a-13 and 13a-15 thereunder because the company did not timely disclose the vulnerabilities and cybersecurity attacks identified by its personnel, which were also alerted by its clients during a six-month period.

[20] Sophie Rohnke, Sarah Pongrace & Mark Schonfeld, *SEC Expands Scope of Internal Accounting Controls to Encompass Companies' Cybersecurity Practices*, Harvard Law School Forum on Corporate Governance, June 29, 2024, https://corpgov.law.harvard.edu/2024/06/29/sec-expands-scope-of-internal-accounting-controls-to-encompass-companies-cybersecurity-practices/

[21] Complaint, *SEC v. SolarWinds, Corp. & Brown*, No. 23-cv-9518 (S.D.N.Y. Oct. 30, 2023), https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-227.pdf

[22] *Id.*

Therefore, the company did not maintain adequate disclosure controls and procedures to timely identify and report cybersecurity incidents.

2. Opinion and Order *SEC v. SolarWinds, Corp. & Brown*

On July 18, 2024, the district court dismissed most of the SEC's claims against SolarWinds and its CISO.[23] The court specifically dismissed the fraud and internal controls charges against the company and its CISO. Nevertheless, the court allowed the claims related to the security statements on the website alleged to be materially false. Importantly, the court held that the SEC's enforcement authority under existing statutes is limited to financial accounting internal controls and does not expand to include each one of the companies' risk management and control policies.

This case marked the first instance wherein the SEC filed an action against a CISO on an individual basis related to alleged cybersecurity breaches. Additionally, it was the first case wherein the SEC accused scienter-based securities fraud in connection with a cybersecurity breach. This case also signified an uncommon occurrence whereby a company contested the SEC's broad interpretation of its authority to file an action for a violation of the "internal accounting controls" provision of the Securities Exchange Act of 1934 stemming from an alleged failure of internal corporate controls—specifically, cybersecurity controls—that extend beyond financial accounting. The court's decision holds notable implications for public companies as they evaluate their cybersecurity risk management, governance, and disclosure practices. Furthermore, beyond the cybersecurity context, the court's ruling established that the SEC is not empowered to file an action for violations of internal accounting controls that are not expressly linked to financial accounting controls.

IV. CONCLUSION

Cybersecurity incidents affecting public companies seem to occur almost daily. Against this backdrop, the SEC has issued extensive guidance regarding the need for cybersecurity related disclosures and internal controls. Additionally, long-standing securities laws and regulations addressing fraud and corporate disclosures apply when companies face cybersecurity incidents. As illustrated by the seven enforcement actions filed from January 2018 to June 2024, the SEC adopts a broad view of liability for cybersecurity-related disclosures and internal controls under the securities laws. Nevertheless, public companies have challenged the SEC's broad view of liability for its cybersecurity-related disclosures and internal controls. The district court ruling in *SolarWings* demonstrates that courts may not necessarily agree with the SEC's broad view of liability under the securities laws, particularly as related to internal controls, wherein the court narrowly interpreted liability for internal controls as referring to controls pertaining to financial accounting and was not necessarily construed to cover a public company's cybersecurity controls. It will be interesting to observe how the SEC and public companies react to future cybersecurity incidents, particularly considering the SEC's aggressive enforcement of cybersecurity-related violations, the *SolarWings* ruling, and the SEC's attempt to expand the scope of internal accounting controls to include cybersecurity controls.

[23] *SEC* v. *SolarWinds Corp. & Brown*, No. 1:23-CV-09518 (S.D.N.Y. July 18, 2024), https://www.nysd.uscourts.gov/sites/default/files/2024-07/SolarWinds%20Opinion%20%28Dkt.%20125%29.pdf

TECHNOLOGY WILL SET YOU FREE, UNLESS YOU ARE IN NON-FOLDING WHEELCHAIR

DR. CHRISTOPHER L. THOMPSON*

I. BACKGROUND AND HISTORY: THE BATTLE

The summer of 1990 saw a watershed moment in United States history. In July of that year, President George H. W. Bush experienced one of the greatest legislative wins of his presidency when he signed into law the Americans with Disabilities Act. In his remarks at the signing ceremony for the Act, President Bush highlighted the historic nature of the legislation.[1] He went on to emphasize the importance of businesses to the Act's success or failure. Additionally, the President pointed out the possibility that American companies seeking a new pool of workers might find them merely by embracing the Act and welcoming the disabled into the workplace.[2]

In many respects, evolving technology has furthered the goals of the Americans with Disabilities Act (ADA). Disabled Americans are now able to participate as both consumers and employees in virtual markets in a way their predecessors could never have dreamed of. However, the same technology has created conflict over whether and to what degree the Act applies to certain technologies and goods and services offered via those technologies. One of these areas of conflict is over whether ride-sharing companies must provide vehicles that are appropriately equipped to transport customers with disabilities, along with their wheelchairs, scooters, or mobility-enhancing equipment. Both Uber and Lyft have been sued for failing to offer wheelchair accessible vehicles in several markets.

To date, the legal results have been mixed. Still, two questions remain despite the courtroom results: 1) Why will these multi-billion-dollar companies[3] not add the required vehicles even if federal law does not require it? 2) Why have states and municipalities not exercised their prerogative to require greater accessibility and accommodation for the disabled? This question is especially vexing in light of the success of laws requiring the companies to provide wheel chair accessible vehicles.

New York City has embarked on a plan appearing to offer a potential solution for other large metropolitan areas. Leveraging the power of its market share, the city has been able to demand ride share companies provide wheelchair accessible vehicles on demand with a strict time window. Obviously, no amount of success in a customer-dense environment can guarantee success

*Associate Professor, Sam Houston State University

[1] Bush, G.H.W..1990, July 26. *Remarks of President George H. W. Bush at the Signing of the Americans with Disabilities Act*. https://archive.ada.gov/ghw_bush_ada_remarks.html.

[2] *Id.*

[3] Wall Street Journal, https://www.wsj.com/market-data/quotes/LYFT (detailing Lyft's $3.21 billion in revenue for 2021 and it's $990.75 million for the June quarter of 2022); Wall Street Journal, https://www.wsj.com/market-data/quotes/UBER/financials (detailing Uber's $14.45 billion in 2021 revenue and $8.07 billion for the June quarter of 2022).

under different circumstances. That being said, it at least offers a roadmap for other large cities to provide increased accessibility for disabled urban dwellers.

A. The Americans with Disabilities Act

The Americans with Disabilities Act (ADA), enacted in 1990, is intended to be the impetus for inclusion and a mechanism for ending discrimination against the disabled.[4] The Act requires business and governmental entities to make accommodations, ensuring their facilities are accessible to the disabled.[5] The Department of Justice (DOJ) is the body charged with issuing any and all regulations necessary to implement the vision of the ADA.[6]

The DOJ was handed a herculean task by the ADA when it made the Attorney General responsible for promulgating any regulations necessary to completely implement the vision of the ADA. The Act also charged the DOJ with assisting those required to comply with the act and enforcing Title III, primarily by giving guidance.[7] However, the size of this burden should be weighed against the resources allocated to the DOJ.

In 2025, that budget exceeded $37.8 billion to be divided among its 11 subgroups.[8] Regarding the suit filed by the DOJ in September 2025, Assistant Attorney General of DOJ's Civil Rights Division Harmeet Dillion said, "[w]e will enforce the ADA's guarantee that people with disabilities have equal opportunity and full participation in all aspects of American society, including transportation."

According to the Centers for Disease Control, as of 2022, twenty-six percent of the U.S. population is living with a disability.[9] With the number of adult Americans at approximately 258 million according to the most recent U.S. census.[10] That is 61 million people, with over 41 million of them being mobility challenged.[11]

With over 41 million Americans living with mobility impairment the matter of their full access and enjoyment of public transportation is vital to their ability to live full and active lives. Further, the average U.S. household featuring a disabled adult requires an income 28 percent greater than a similarly situated household without a disabled member to maintain an equivalent standard of living.[12] This is obviously an important issue, not just ethically or morally but economically. A 2022 study exploring the potential economic impacts of addressing underemployment by disabled persons via improved transportation provides an excellent view into

[4] 42 U.S.C. § 12101 (b)(1); *Olmstead v. L.C. ex Rel. Zimring*, 527 U.S. 581, 589 (1999).
[5] 42 U.S.C. § 12101 (b) (1-4).
[6] *See* 42 U.S.C. 12186 (b).
[7] *United States v. AMC Entertainment, Inc., F.3d 760 (9th Cir. 2008).*
[8] U.S. Department of Justice. https://www.justice.gov/jmd/media/1342656/dl?inline.
[9] Centers for Disease Control. https://www.cdc.gov/ncbddd/disabilityandhealth/infographic-disability-impacts-all.html.
[10] United States Census Bureau, https://www.census.gov/library/stories/2021/08/united-states-adult-population-grew-faster-than-nations-total-population-from-2010-to-2020.html.
[11] *Id*; Centers for Disease Control, https://www.cdc.gov/ncbddd/disabilityandhealth/infographic-disability-impacts-all.html#:~:text=11.1%20percent%20of%20U.S.%20adults,concentrating%2C%20remembering%20or%20making%20decisions.
[12] Nanette Goodman, Michael Morris, Zachary Morris, Stephen McGarity, *The Extra Costs of Living with a Disability in the U.S.—Resetting the Policy Table*, October 2020, National Disability Institute. https://www.nationaldisabilityinstitute.org/wp-content/uploads/2020/10/extra-costs-living-with-disability-brief.pdf.

why every person, company, and government subdivision has a stake in this issue.[13] The researchers found that improving transportation availability to and from work for disabled individuals could allow just 15 percent more of those people to enter the work force[14] it would result in a significant jolt to the U.S. economy.[15] The said jolt would consist of 4.4 million jobs for the disabled and 9.2 million total jobs created, which would in turn increase the U.S. GDP by 3.8 percent or $868 billion, all while generating nearly $93 billion in total federal tax revenue.[16]

II. The ADA and Transportation

The ADA requires compliance from both public and private transportation providers.[17] Generally speaking, this requires allowing disabled persons to fully and equally enjoy public transportation, even if it is provided by a private company.[18] However, there is a carve-out for taxi companies.[19]

A privately operated taxi service is not required to offer ADA-compliant cabs unless it buys or leases vehicles other than passenger automobiles.[20] Essentially, as long as a cab company only maintains a fleet of sedans, it never has to offer accessible vehicles.[21] In this context, a wheelchair-accessible vehicle is one that "accommodates a passenger using a wheelchair or other personal mobility device who needs a ramp or lift to enter or exit the vehicle."[22] When a company purchases any type of vehicle other than an "automobile," it must be accessible unless the company can demonstrate it offers an equivalent service.[23] Further, a private taxi service cannot discriminate against a disabled person by refusing them service, refusing to help with loading their wheelchairs or equipment or by charging them a higher fare.[24]

In many markets, the rise of ride-sharing companies has made traditional taxi services largely irrelevant. Nationwide, between the first quarter of 2014 and the first quarter of 2018, the percentage of business travelers choosing ride-sharing over taxis and rental cars increased from 6% to 70.5%.[25] Almost immediately, complaints arose that ridesharing companies were not complying with the ADA.

---

[13] D. Modicamore, G. Voigt, D. Clark, J. Murphy, E. Layman, *Economic Impacts of Removing Transportation Barriers to Individuals with Disabilities Through Autonomous Vehicle Adoption,* Dec. 30, 2022, National Disability Institute. https://www.nationaldisabilityinstitute.org/reports/autonomous-vehicle-adoption/. (the study goes about resolving the issue of transportation of disabled persons from another angle, namely the adoption of self-driving vehicles but the numbers are helpful in this context as well).

[14] essentially just reducing the amount of disable people who are unemployed by 15 percent.

[15] D. Modicamore, G. Voigt, D. Clark, J. Murphy, E. Layman, Economic Impacts of Removing Transportation Barriers to Individuals with Disabilities Through Autonomous Vehicle Adoption, Dec. 30, 2022, page 16, National Disability Institute. https://www.nationaldisabilityinstitute.org/reports/autonomous-vehicle-adoption/.

[16] *Id.*

[17] 42 USC § 12184;

[18] *Id.*

[19] www.adata.org.

[20] *Id.*

[21] *Id.*

[22] https://www.lawinsider.com/dictionary/wheelchair-accessible-vehicle#:~:text=Define%20Wheelchair%20Accessible%20Vehicle.%20means%20a%20vehicle%20compliant,of%2049%20C.F.R.%20Part%2038.1%20%E2%80%93%2038.39.%E2%80%9D.%20Browse.

[23] *Id.*

[24] *Id.*

[25] Michael Goldstein, *Dislocation and Its Discontents: Ride-Sharing's Impact on The Taxi Industry*, June 8, 2018, Forbes. https://www.forbes.com/sites/michaelgoldstein/2018/06/08/uber-lyft-taxi-drivers/?sh=225cb51759f0.

A. *Legal Issues*

Uber has been accused of violating the ADA in several different ways. These include charging disabled passengers higher fares than their non-disabled counterparts[26], and drivers screaming at service dog-dependent people and refusing to allow them inside their vehicle.[27] Lyft has not been immune to similar suits and has been sued frequently as well.[28] In September of 2025, Uber was sued by the U.S. Department of Justice because its drivers, allegedly, regularly refusing to pick up disabled individuals, charging passengers cleaning fees related to service animal hair, and charging disabled people "cancellation fees" when drivers wrongfully denied them service.

A favorite legal position frequently taken by both Uber and Lyft is that they are not a taxi or transportation company. Instead, they argue they are merely "technology platforms" connecting drivers and passengers.[29] This is essentially their "throw-down argument" in legal disputes spanning such disparate issues as the independent contractor status of their drivers to ADA disputes.[30]

This self-identification is crucial to their business model because it allows them (in their own minds at least) to avoid a myriad of legal obligations it would otherwise have to bear. These burdens include state and local regulations on taxi companies, state and federal labor laws such as minimum wage and overtime pay, withholding and remitting payroll tax, Medicare and Social Security, as well as the responsibility to comply with the ADA.[31] However, the companies have not found this argument universally successful and have at times found it necessary to settle suits rather than face trials.[32] For example, Uber settled a suit alleging it discriminately charged disabled individuals a $0.60 wait time fee to the tune of approximately $2.2 million.[33]

Another common argument put forth by ridesharing companies, which has been for the most part successful, is that providing WAV in certain localities would be cost-prohibitive and

---

[26] Mary-Ann Russon, *Uber Sued by Justice Department for Overcharging Disabled People*, November 11, 2021. https://www.bbc.com/news/business-59242866.

[27] *National Federation of the Blind California v. Uber Technologies, Inc.*, 103 F.Supp. 3d 1073, (N.D. California, 2015).

[28] *E.g. McPhail v. Lyft, Inc.,* 2015WL1143098, (W.D. Texas); *e.g* Kerr, D. *Lyft to Pay $40,000 Fine Over Claims It Denied Disabled Passengers Rides*, June 22, 2020. https://www.cnet.com/tech/mobile/lyft-pays-40000-fine-over-claims-it-denied-disabled-passengers-rides/.

[29] *See* Joel Rosenblatt, *Uber's Business Model May Depend on Convincing the World Drivers Aren't Part of Their "Core Business"*, Time, September 12, 2019. https://time.com/5675637/uber-business-future/; *see also* Melissa Locker, *Lyft's Response to ADA Lawsuit: Sorry We're Not in the "Transportation Business",* Fast Company, May 3, 2019. https://www.fastcompany.com/90343921/lyft-claims-its-not-a-transportation-company-to-avoid-ada-compliance; *Equal Rights Center v. Uber Technologies*, 525 F.Supp.3d 62, 84 (D.C.Cir., 2021).

[30] *See Id; see also* Kelly Phillips Erb, *Worker or Independent Contractor? Uber Settles Driver Claims Before Disappointing IPO*, Forbes, May 13, 2019. https://www.forbes.com/sites/kellyphillipserb/2019/05/13/worker-or-independent-contractor-uber-settles-driver-claims-before-disappointing-ipo/; *see Equal Rights Center v. Uber Technologies, Inc.*, 525 F.Supp.3d 62, 84 (U.S. D.C., 2021).

[31] Bryan Casey, Uber's Dilemma: How the ADA May End the On Demand Economy, 12 U.Mass. L. Rev. 126, 140-141 (citing Cotter v. Lyft and Carmel DeAmicus, *Uber Could Have to Pay an Additional $209 Million to Reclassify its Drivers in California,* https://www.vox.com/2015/7/14/11614646/uber-could-have-to-pay-an-additional-209-million-to-reclassify-its*)*

[32] *E.g.* Attorney General James Secures $328 Million from Uber and Lyft for Taking Earnings from Drivers." New York State Attorney General. November 2, 2023. https://ag.ny.gov/press-release/2023/attorney-general-james-secures-328-million-uber-and-lyft-taking-earnings-drivers.

[33] Madeline Halpert, *Uber Will Pay Over $2 Million to Settle Claims It Overcharged Customers With Disabilities*, Forbes, July 18, 2022. https://www.forbes.com/sites/madelinehalpert/2022/07/18/uber-will-pay-over-2-million-to-settle-claims-it-overcharged-customers-with-disabilities/?sh=652b8148727b.

hence not a reasonable accommodation under the ADA. So, for example, while disabled persons in need of a WAV in New York City, Boston, Houston, or Los Angeles can get one on demand via Uber's UberWAV program, that very same person, if they were visiting New Orleans, could not.[34] The argument hinges on the "reasonable accommodation" verbiage in the Act. Essentially questioning the reasonableness of requiring the companies to spend large sums of money in small markets.[35]

While the ADA is not flawless it includes a very important feature demonstrating the care its drafters took to provide federal protection for the disabled without impeding states from doing even more.[36] The text of the ACT made it clear from the beginning that it was not intended to preempt states or cities from making their own laws or ordinances requiring even greater accessibility.[37] The so-called "Relationship Clause' states

> (b) Relationship to other laws
> Nothing in this chapter shall be construed to invalidate or limit the remedies, rights, and procedures of any Federal law or law of any State or political subdivision of any State or jurisdiction that provides greater or equal protection for the rights of individuals with disabilities than are afforded by this chapter. Nothing in this chapter shall be construed to preclude the prohibition of, or the imposition of restrictions on, smoking in places of employment covered by subchapter I, in transportation covered by subchapter II or III, or in places of public accommodation covered by subchapter III.[38]

The Relationship Clause provides the means for both states and cities to fulfill the great promise of the ADA. It clearly gives political subdivisions the ability to make laws, rules, and regulations requiring ride-sharing companies to provide WAVs on demand or at least to make them more readily available. Notably, New York has created a system doing exactly that.[39]

III: The New York City Solution

Starting in 2019, New York City's Taxi and Limousine Commission (TLC) put in place new accessibility rules for what it terms for-hire vehicles (FHV).[40] The TLC's definition of an FHV includes ride-sharing companies, including Uber and Lyft. These rules are noteworthy and might one day provide a road map for other cities to require greater accessibility.

The rules enacted by the TLC require for-hire vehicle companies to improve accessibility and gives them two options for doing so.[41]

---

[34] *See* Anthony Warren, *Ninth Circuit says Uber Doesn't Have to Provide Wheelchair Accessible Ride Service in Jackson, New Orleans*, July 26, 2022. https://www.wlbt.com/2022/07/26/ninth-circuit-says-uber-doesnt-have-provide-wheelchair-accessible-ride-service-jackson-new-orleans/.
[35] *Id.*
[36] Barry Fagin, *The ADA is a Terrible Law and Should be Repealed*, The Gazette, Nov. 14, 2019. https://gazette.com/opinion/column-the-ada-is-a-terrible-law-and-should-be/article_7ee5be86-062d-11ea-96e6-035599668baf.html.
[37] 42 USCA § 12201 (b).
[38] *Id.*
[39] *See* Rule 59 B-17, Title 35, Rules of the City of New York.
[40] Rule 59 B-17, Title 35, Rules of the City of New York.
[41] *Id.*

The first option is known as the "Trip Mandate Rule." It requires a fixed percentage of each FHV company's dispatched cars to be WAVs, regardless of whether one was requested.[42] Cleverly, the required percentages began at a low 5% in January 2019 and gradually increased up to 25% between July 2022 and June 2023.[43]

Option two is the "Central Dispatch Exception." It allows FHV companies to affiliate with central dispatchers to send WAVs on demand, subject to certain wait time requirements.[44] The mandated wait time percentages began in June 2019 with requiring 60% of calls to be answered by a WAV within 15 minutes and 90% of calls to be answered within 30 minutes.[45] This ratcheted up in 2020 to 80% within 15 minutes and 90% within 30 minutes.[46] By June 2021, 80% of calls were to be answered within 10 minutes and 90% within 15 minutes.[47]

The new rules paid dividends almost immediately, with the number of WAVs being operated for hire in the city going up 1000% from June 2018 to the end of June 2019.[48]

During the second-year evaluation period spanning July 2019 to September 2020, of the 767 companies required to comply with the rules, 267 chose the trip mandate and 500 chose the central dispatch exception.[49] Percentage-wise, 98% of all the trips serviced by FHVs were done by companies choosing the central dispatch option, with only 2% being serviced by those opting for the trip mandate.[50]

The third and most recent evaluation period, spanning July 1, 2023, to June 30, 2024, showed even greater success with the number of WAV's available ballooning.[51] Fiscal 2024 ended with 5,800 WAV working as for-hire vehicles, up from 339 in January 2019.[52]

It is quite apparent that the central dispatch exception is the more important and effectual that the trip mandate rule. In June 2019, across the participating companies, including Uber and Lyft, 74% of requests for a WAV were answered in less than 15 minutes, and 94% were answered in less than 30 minutes, both of which exceeded the minimum requirements.[53] A year later, 62.33% of requests were answered in less than 10 minutes, 82.66% within 15 minutes, and 95.66% within 30 minutes, all of which well exceed the minimum requirements.[54] In the most recent evaluation

---

[42] Rule 59 B-17(c), Title 35, Rules of the City of New York; *see* For-Hire Vehicle Wheelchair Accessibility Evaluation Report, Year 2, New York Taxi & Limousine Commission, May 2021. https://www.nyc.gov/assets/tlc/downloads/pdf/fhv_wheelchair_accessibility_report_2020.pdf.

[43] see For-Hire Vehicle Wheelchair Accessibility Evaluation Report, Year 2, page 4, New York Taxi & Limousine Commission, May 2021; It should be noted that the time period of the evaluation was extended by three months during the 2019-2020 period to compensate for the effects of Covid-19.

[44] Rule 59 B-17(f), Title 35, Rules of the City of New York.

[45] Rule 59 B-17(f), Title 35, Rules of the City of New York.

[46] *Id.*

[47] *Id.*

[48] FHV Compliances with Wheelchair Accessibility Requirements, page 2, New York Taxi & Limousine Commission, September 2019.

[49]see For-Hire Vehicle Wheelchair Accessibility Evaluation Report, Year 2, page 5, New York Taxi & Limousine Commission, May 2021.

[50] *Id.*

[51] For-Hire Vehicle Wheelchair Accessibility Evaluation Report, Year 6, page 1, New York Taxi and Limousine Commission, June 2024.

[52] *Id.*

[53] FHV Compliances with Wheelchair Accessibility Requirements, page 10, New York Taxi & Limousine Commission, September 2019.

[54] For-Hire Vehicle Wheelchair Accessibility Evaluation Report, Year 2, page 6, New York Taxi & Limousine Commission, May 2021.

period, 88% of passengers requesting a WAV were picked up within 10 minutes of requesting a ride.[55]

Even one of the TLC's most ardent critics, the non-profit New York Lawyers for Public Interest (NYPLI), found in an independent study it carried out that the new rules have been very successful in some key metrics.[56] First, regarding vehicle availability as measured by the rate of success in finding an available vehicle, the major companies, including Lyft, Uber, and Via the rate of success in connecting with a WAV was either equal to or better than the success rate of users attempting to find a non-WAV.[57] Second, FHV's must charge the same fare for a trip in a WAV as they would charge for the same trip in a non-accessible vehicle.[58] New York's providers, as a group, were very successful at meeting this mandate as well.[59]

IV: CONCLUSION

The New York City solution is by no means a perfect one. However, the demonstrably positive results it produced lead one to the obvious question of why other states have not followed suit. For Americans, depending on greater access to transportation to improve their lives as well as their work prospects, the matter is urgent. It is arguably even more urgent for Uber and Lyft themselves, both of whom in 2023 notched major milestones.

In 2023, for the first time, Uber turned a profit while Lyft managed to make more money than it spent.[60] Uber then went on to make $6.9 million in profits in 2024.[61] Also in 2024, Lyft had its first profitable year ever. As both companies mature, there is a strong argument to be made that these companies should take the initiative and voluntarily invest the capital they spend every year to litigate and settle lawsuits brought by and on behalf of mobility-challenged people to offer WAVs in every market that it is conceivably possible. The companies should view this simultaneously as an investment and a prophylactic move to avoid lawsuits.

[55] For-Hire Vehicle Wheelchair Accessibility Evaluation Report, Year 6, page 1, New York Taxi and Limousine Commission, June 2024.
[56] NYPLI's study results bear this out however the organization continues to call for increased accessibility and has exposed higher fees charged by some companies for trips in WAVs.
[57] Continuing to Be Left Behind, page 7-8, NYPLI, 2021_Continuing-to-be-Left-Behind-Report.pdf (nylpi.org)
[58] Continuing to Be Left Behind, page 11, NYPLI, 2021_Continuing-to-be-Left-Behind-Report.pdf (nylpi.org).
[59] *Id.*
[60] Preetika Rana, *Have Uber and Lyft Finally Found a Way to Make Ride-Sharing Profitable?* Wall Street Journal, February 15, 2024. https://www.msn.com/en-us/money/companies/have-uber-and-lyft-finally-found-a-way-to-make-ride-sharing-profitable/ar-BB1ijwfh.
[61] Uber. (Feb. 5, 2025) *Uber Announces Results for Fourth Quarter and Full Year 2024*, [Press Release]. https://investor.uber.com/news-events/news/press-release-details/2025/Uber-Announces-Results-for-Fourth-Quarter-and-Full-Year-2024/default.aspx.

3D: DECONSTRUCTING DEFAMATION DAMAGES

SAMEER S. SOMAL*
WILLIAM CHOSLOVSKY

I. INTRODUCTION

Recent high-profile and high-value defamation cases against politicians and celebrities have garnered significant media attention, thrusting the topic of defamation into the news headlines. In January 2024, a jury found Donald Trump guilty of sexual abuse and defamation, awarding Jean Carroll $18.3 million in compensatory damages and an additional $65 million in punitive damages, totaling to $83.3 million.[1] This followed a 2023 case by Carroll, which had also resulted in damages. In 2023, Rudy Giuliani was ordered to pay $148 million in damages to two Georgia election workers whom he falsely accused of voter fraud—part of efforts that also have Giuliani facing criminal charges.[2]

In other politically sensitive cases, Alex Jones—who peddled conspiracy theories and misinformation about the tragic 2012 Sandy Hook school shooting in Connecticut—was found liable for $1.5 billion in damages.[3] The right-leaning media network Fox News Channel and its corporate parent, Fox Corp. recently settled a defamation case brought by Dominion Voting Systems, agreeing to pay $787.5 million—one of the largest ever publicly disclosed monetary settlements in the U.S.[4] Fox admitted it had broadcast factually incorrect statements about Dominion's voting machines following the 2020 presidential election. Dominion had previously sought $1.6 billion in damages.[5]

Of course, Hollywood and the film industry have seen similar cases. Johnny Depp and his ex-wife Amber Heard sued each other for defamation, with Depp prevailing and receiving a $15-million defamation award in a case that grabbed and held public attention on the news and social media. [6] The suit placed the two on a growing list of actors and other celebrities who have sued individuals and publications for defamation, including Meghan Markle and Prince Harry, Tom Cruise, Sharon Stone, Cameron Diaz, and Scarlett Johansson.

Such overwhelming verdicts reflect a sea change in defamation law. Whereas previously, damages from reputational harm were based on tangible factors that could be easily calculated (such as newspaper circulation numbers), courts today struggle to value compensatory damages stemming from viral reputational harm in the digital age. Social media algorithms can propagate material that agrees with a user's opinions and contribute to the spread of false information.

---

* CFA Charter holder, Georgetown University
[1] Carroll v. Trump, No. 23-793 (2d Cir. 2024)
https://www.afslaw.com/perspectives/alerts/big-audience-justifies-big-damages-defamation-lawsuit-against-trump
[2] Freeman et al. v. Giuliani, 1:23-cv-03754, (D.D.C. 2023
[3] Heslin et al. v. Jones et al., No. 23-3035 (S.D. Tex. 2023)
[4] US Dominion, Inc. et al. v. Fox News Network, LLC, N21C-03-257; N21C-11-082, (Del. Super. Ct. 2023).
[5] Supra. at *15.
[6] John C. Depp, II v. Amber Laura Heard, CL-2019-0002911, (Va. Cir. Ct. 2022).

Because misinformation is repeated and quickly shared, it can increase reputational damage at geometric levels.[7]

The compensatory and punitive damages awarded as a result of proven defamation can seem astronomical, and at first glance, there may appear to be little rhyme or reason for such titanic valuations. However, verifiable valuation principles are emerging. Of course, given varying laws across multiple jurisdictions, there is no simple, cookie-cutter formula for assessing damages in defamation cases. Nonetheless, the legal industry is striving to achieve answers.

In the absence of a concrete, universal formula, plaintiff attorneys often go to elaborate efforts to detail damages in cases: assessing the spread of defamatory statements, calculating economic damages such as lost wages and business opportunities, and pushing for punitive damages aimed at discouraging repeated defamatory behavior.[8] Legal teams are also bringing in expert witnesses who are able to explain the technical details of these assessments in reports and testimony to judges and juries.

This article deconstructs calculations of damages in defamation cases and considers the defamation law behind these valuations.

II. BASICS OF DEFAMATION

Defamation involves public communication that injures the reputation of another individual or group. Broadly, defamation is divided into two types: *slander* for oral statements and *libel* for written statements. Though the nuances of defamation vary by jurisdiction, the essence is similar: to introduce a case of defamation, a plaintiff must establish four elements:

1. The defendant made a false statement of material fact about the plaintiff.
2. The false statement was made or published to a third party.
3. The statement is not subject to privilege.
4. The statement caused damage or harm to the defendant's reputation.[9]

For example, in the Illinois case of *Solaia Technology LLC v. Specialty Publishing Co.* (2006),[10] the plaintiff alleged defamation over infringement claims regarding a patent dispute. In its analysis, the Supreme Court of Illinois stated that "a defamatory communication violates an individual's right to a good reputation and gives rise to a cause of action to recover damages for the violation."[11] The opinion added, "A defamatory statement becomes actionable when it is communicated to a third party and understood by that person as being defamatory."[12]

---

[7] Vishika Dhalia and Raghwender Vasisth, Defamation in Digital Crossfire: Algorithms, Social Media, Blockchain and Global Jursdiction, The Legal Journal on Technology (2025).

[8] Punitive Damages in Defamation Litigation, Yale Law Journal, Vol. 64, Issue 9 (1955).

[9.] Restatement (Second) of Torts § 558 cmt. a (Am. Law Inst. 1977).

[10.] Solaia Technology, LLC v. Specialty Publishing Company, 221 Ill.2d 558, 852 (Ill. Sup. Ct. 2006). (For the sake of convenience, we cite Illinois cases, as Illinois generally reflects the basic principles of defamation, though nuances exist especially when the defamation victim is a public figure).

[11.] Supra. at 36.

[12.] Supra. at 37.

A. Defamation Per Quod and Defamation Per Se

To understand how damages are calculated, we must first look at the types of statements the law covers: defamation *per se* and defamation *per quod*. The difference lies in the severity of the false defamatory statements.

1. Defamation *per se*

Defamation *per se* is defamation "on its face," that is, false statements that are obviously harmful, such as claiming a person committed a serious and heinous crime, cannot perform their job, or is an adulterer. Ultimately, as expressed in *Owen v. Carr* (1986), a statement is defamatory *per se* if it is "so obviously and naturally harmful to the person to whom it refers that a showing of special damages is unnecessary."[13]

2. Defamation *per quod*

Defamation *per quod* involves slander or libel that is less obvious, meaning the plaintiff must prove the false statement(s) caused damage. This includes less obviously injurious statements, such as claiming one's neighbor never cuts his grass or fails to pay his church tithes, or statements in which the plaintiff is unable to prove actual malice on the part of the defendant. An example of this is *Barteck v. Personal Finance Co. of Toledo*, 60 Ohio App. 197, 20 N. E. (2d) 259 (1938). [14] The Plaintiff alleged that she had been defamed by the defendant and claimed damages. Here, the court observed: "It is not and is not claimed to be a cause of libel per se, but libel per quod. Special damages must be and are alleged. "

The primary difference between statements that are defamation *per quod* and those that are defamation *per se* involves the assessment of damages. In short, for statements that are deemed defamation *per quod*, the plaintiff must prove tangible damages by providing concrete evidence in the form of records detailing actual harm. [15] The U. S. Supreme Court has emphasized that plaintiffs must provide proof of actual damages in *per quod* cases to avoid creating a chilling effect on the free expression of ideas in public discourse. [16]

In contrast, when statements are so egregious that they are categorized as defamation *per se*, damages do not need to be proven. For defamation *per se* plaintiffs, most states allow presumed damages, meaning damages are presumed without evidentiary requirements. The court in *Winters v. Greeley*[17] explained, "Although there is no scale by which to measure the monetary value of reputation, goodwill, or loss of esteem, the law nevertheless recognizes the impairment of reputation and community standing, loss of esteem, personal humiliation, and anguish as actual injuries that necessarily flow from a *per se* defamatory statement. "[18]

[13.] Owen v. Carr,113 Ill. 2d 273, 277, 497 N.E.2d 1145 (Ill. Sup. Ct. 1986). See also Costello v. Capital Cities Communications Inc., 125 Ill.2d 402, 414 (Ill. Sup. Ct. 1988) and Green v. Rogers, 234 Ill. 2d 478, 491-92 (Ill. Sup. Ct. 2009), and *Bryson v. News America Publications, Inc.* (1996).

[14] Barteck v. Personal Finance Co. of Toledo, 60 Ohio App. 197, 20 N. E. (2d) 259 (1938).

[15.] See *Economic Damages in Defamation*, 42 Am. Jur. 2d Damages 45 (2023).

[16.] Gertz v. Robert Welch, Inc. 418 U.S. 323, 350 (1974).

[17.] Winters v. Greeley, 189 Ill. App. 3d 590, 598 (Ill. Sup. Ct. 1989).

[18.] Supra.

B. The Threat of Online Defamation

The internet has created a new landscape where opinions can be shared with abundant ease, leading to a rise in defamation and damages caused. Social media complicates that landscape further, adding a new dimension to the problem.

By allowing an outlet for expression in which users can publish statements without the traditional oversight of editors, digital speech itself presents new challenges to the conventional definition of defamation and the role of social media companies in monitoring content. Given its tendency toward a casual and hyperbolic tone, particularly on social media pages, some state courts have tended to regard the conversational nature of "internet speech" on some platforms as unable to be treated as actionable statements of fact, thereby distinguishing it from statements issued by traditional media outlets.[19] However, some rulings have sought to apply conventional defamation principles to online statements. In *SI03, Inc. v. Bodybuilding.com* (2008), for instance, a U.S. District Court in Idaho emphasized that users must ensure the accuracy of their online statements to avoid defamation charges.[20]

Complicating the issue further is the fact that many online defamatory statements are expressed anonymously or pseudonymously, and courts have long upheld a person's right to anonymous speech.[21] On social media, however, an anonymous user can make false, defamatory statements in seconds with the click of a mouse, and the content can spread around the world instantly, often causing considerable reputational harm before the victim even learns of the situation.[22]

Online defamation includes social media posts and comments on sites such as Facebook, Instagram, X (Twitter), or LinkedIn. Both public figures and private individuals have been defamed by factually incorrect or incomplete information regarding alleged infidelity, criminal activities, or other embarrassing behavior. This harm may be caused by malicious intent, but can also happen from simple negligence resulting from failure to fact-check information.[23] Defamation cases have defined distinctions between actual malice and a negligence standard, and between public figures and private individuals.[24] Some instances of defamation are then shared and re-shared on multiple platforms and media, including by traditional media outlets as well as chat forums, podcasts, and others.

Users may post false or malicious negative reviews of businesses or individuals on sites such as Yelp and Amazon, and courts have generally considered traditional websites and online review sites as more serious sources of factual information than chat rooms, blogs, and bulletin boards.[25] Moreover, negative posts and reviews can impose a secondary negative impact on an entity's search engine results, potentially leading to additional damages.[26]

[19.] *See eg.,* Feld v. Conway, 16 F. Supp., 3d 1, 4 (D. Mass 2014); Jacobus v. Trump, 51 N.Y.S.3d 330, 339 (N.Y. Sup. Ct. 2017).

[20.] SI03, Inc. v. Bodybuilding.com, LLC, No. CV 07-6311-EJL (U.S. Distr. Ct. Idaho 2008).

[21.] Talley v. California, 362 U.S. 60 (1960).

[22.] Daniel Keats Citron, *Hate Crimes in Cyberspace*, 61-62 (2014).

[23.] N.Y. Times Co. v. Sullivan, 376 U.S. 254, 267 (1964).

[24.] Gertz v. Robert Welch, 418 U.S. 323, 347 (1974).

[25.] Hadley M. Dreibelbis, *Social Media Defamation: A New Legal Frontier Amid the Internet Wild West*, Duke Journal of L. & Pub. Pol'y, Vo. 16, 273 (2021).

[26.] Siva Vaidhyanathan, The Googlization of Everything (and Why We Should Worry) 20-21 (2011).

Other cases involve impersonation, in which the perpetrator assumes another person's identity for the purpose of attracting negative attention. This can range from creating a fraudulent social media account under another's name and then using the account to share content designed to harm the person's reputation, or using deep fake technology to imitate the likeness or voice of a person to achieve similar goals.[27]

The result of online defamation is twofold: The damage spreads much farther and wider, and the process of assessing and proving damages in court becomes more technical and complex, forcing courts to examine the particular platform or website in which the statement was published, as well as the statement's overall purpose and context.[28] To help quantify the level of damage inflicted on a victim, courts are now tasked with considering factors such as geographic spread or virality metrics, as the number of shares and engagement rates may help determine the degree of a message's influence.[29]

C. Elements of Defamation Damages

Regardless of whether a case is *per quod* or *per se*, similar damage elements and categories apply. Generally, there are five types of potential defamation damages:

1. Economic Damages
2. Physical Harm Damages
3. Emotional Harm Damages
4. Rehabilitation Repair Damages
5. Loss of Reputation Damages

The first four are relatively straightforward, at least conceptually. Briefly:

1. Economic Damages

Economic damages compensate plaintiffs for financial losses caused by defamatory statements, which may include lost income, diminished future income, or lost business opportunities. If defamation causes someone to lose their job, the loss of income is considered economic damage. Though the concept is straightforward, calculating or estimating the loss is often not.

For instance, calculating how long someone's earnings may be diminished in the future because of defamation requires complex estimation and certain assumptions, often leading to a range of values. Likewise, even if the victim does not lose employment as a result of defamation, the victim's future opportunities for promotion or new positions may be limited; that, too, is subject to calculation. When calculating a range of damages based on loss of future income, the numbers should be expressed as present value (to account for the time value of money) and reflect anticipated future inflation. In other words, inflation must be incorporated into the discount rate used in present value calculations—often called a "real discount rate."

[27.] Sarah H. Jodka, *Manipulating Reality: the Intersection of Deep Fakes and the Law*. Reuters, https://www.reuters.com/legal/legalindustry/manipulating-reality-intersection-deepfakes-law-2024-02-01 (2024).

[28.] Dreibelbis at 257-269.

[29.] Ji Won Kim, They Liked and Shared: Effects of Social Media Virality on Perceptions of Message Influence, Computers in Human Behavior, Vol. 84, 153-161 (2024).

As for the plaintiff's income, damages suffered are generally measured by the difference between the plaintiff's projected earnings if the defamation did not occur and the plaintiff's actual earnings. This process involves evaluating their historical earnings and using them to calculate possible future earnings, often a complex and painstaking process. (Again, the present value of these future earnings should use a real discount rate.) In addition to W-2s and tax filings, legal teams may also look at the state of the economy, the condition of the plaintiff's industry, the plaintiff's business calendar showing a possible decline in business, and the earnings of others involved in the same occupation.

In *Harte-Hanks Communications, Inc. v. Connaughton*, the U.S. Supreme Court affirmed $200,000 compensatory damages for the plaintiff's failed political campaign and business reputation, emphasizing the case report's detailed evidence concerning loss of opportunities such as withdrawn campaign support. [30] Conversely, in *Brady v. Ottaway Newspapers,* the court denied damages in part because the plaintiff, a police chief, could not show with definitive evidence that defamation caused any specific losses, such as loss of promotions or early retirement.[31]

Although the burden of evidence of *per quod* cases can prove complicated for plaintiffs and their attorneys, calculating presumed damages in *per se* cases can also be complex, given the intangible nature of reputation, prompting some to call for minimum awards in cases of defamation *per se*.[32]

2. Physical Harm Damages

Defamation deals with the spoken and written word, so it's easy to overlook physical damages. Yet, the old saying, "Sticks and stones will break my bones, but words will never hurt me," does not apply to defamation. Even though the main damage in defamation cases involves harm to reputation, compensation may be due if the defamation causes stress or other factors that result in physical health problems. For instance, if someone suffers high blood pressure or an ulcer because of a defamatory statement, that is, of course, physical damage. Likewise, a reduced libido or loss of hair because of a defamatory statement is physical harm.

In *Lerman v. Flynt Distributing Co.*, the plaintiff successfully argued that, in addition to emotional anguish, she had suffered from ulcers and insomnia following a false magazine story. The jury decided to award damages for her injuries. In its opinion, the federal court pointed out that the evidence clearly tied Lerman's ulcers and related health issues to the defamation, and that a private person like Lerman did not have to prove malice. [33] In a Maryland case, *Bowden v. Caldor*, the plaintiff proved that he had suffered physical ailments following a false public accusation, causing him to experience a nervous breakdown that required hospitalization. Medical experts testified that the false allegation led to the plaintiff's worsening physical health, including acute anxiety and stress-related symptoms. The jury decided that the plaintiff was entitled to $110,000 in compensatory damages, which included harm to his reputation as well as his health, and an appellate court upheld the verdict.[34]

[30.] Harte-Hanks Communications, Inc. v. Connaughton, 491 US 657 (U.S. Supr. Ct. 1989).

[31.] Brady v. Ottoway Newspapers, 84 A.D.2d 226445 N.Y.S.2d 786 (N.Y. Sup. Ct. 1981).

[32.] Steven A. Krieger, Defamation Per Se Cases Should Include Guaranteed Minimum Presumed Damage Awards to Private Plaintiffs, San Diego L. Rev. Vol. 58, 641 (2021).

[33.] Lerman v. Flynt Distributing Co., Inc., 789 F.2d 164 (2d Cir. 1986).

[34.] Bowden v. Caldor, 710 A.2d 267, 350 Md. 4 (Md. Ct. of App. 1998).

Courts usually request medical proof to back up physical harm claims, and calculate a dollar figure in turn. Answering questions such as how much an ulcer has damaged a person is often more art than science, subject to broad interpretation. Legal teams must quantify and provide evidence for these issues, often in the form of expert witness testimony. As with emotional harm, medical experts must distinguish pre-existing conditions from defamation-related ailments.[35] Plaintiffs may also include corroborating testimony from family or colleagues to help substantiate claims.[36]

3. Emotional Harm Damages

Defamation victims often suffer from a range of emotional distress issues that can result in real medical and psychological problems. Twenty years ago, most courts focused primarily on economic damages, but today the only question regarding emotional damages is how to quantify them.[37]

There is often a high level of mental anguish from the stigma associated with defamation. This often stems from the awareness that friends, family, neighbors, and colleagues know about defamatory content and the constant need to explain. As some experts have noted, "Some allegations are so heinous that any reasonable person would accept that they are inherently distressful [like] 'child molester,' 'sexual predator,' and 'racist' are hot-button accusations.[38]

The landmark case *Gertz v. Robert Welch, Inc.* (1974) helped establish precedent regarding emotional distress claims in many jurisdictions.[39] The U.S. Supreme Court decided that states could base awards on elements other than injury to reputation, specifically listing "personal humiliation, and mental anguish and suffering" as examples of harm which may be compensated consistently with the Constitution upon a showing of fault.[40] When defamation causes mental anguish—as it often does—evidence can be collected similar to documenting lost wages and business opportunities. Given this evidentiary requirement, victims should begin collecting evidence from the start. Common evidence includes medical reports from therapists and psychiatrists, prescriptions for medications, and documentation of emergency room and hospital visits.

In a high-profile case, Las Vegas casino billionaire Steve Wynn filed a slander suit against Joe Francis, creator of the Girls Gone Wild adult video empire.[41] Wynn successfully argued that he experienced mental anguish over worries that his employees could suffer if his casino suffered because of the defamation, leading the jury to award him $3 million in damages for emotional distress, which was later reduced to $2 million.

In Minnesota, a state senator alleged that a citizen defamed her by accusing her of theft on signs placed throughout her district in the weeks leading up to the election, which the senator lost.[42] In the trial, the senator offered testimony that she "experienced severe stress, manifested by headaches and sleeplessness," and that the act of libel had placed additional strain on her children

---

[35.] David A. Anderson, *Reputation, Compensation, and Proof*, 25 Wm. & Mary L. Rev. 747, 763 (1984).

[36.] Lyrissa Lidsky, *Where's the Harm?*, 71 Wash. & Lee L. Rev. 1101, 1123 (2014).

[37.] Rodney A. Smolla, *Law of Defamation,* (2d ed. 2023).

[38.] Nicholas Carroll, *Emotional Distress Damages in Defamation Cases,* American Bar Association (2019).

[39.] Gertz v. Robert Welch, Inc., 418 u.S. 323, 346 (1974).

[40.] Supra

[41.] Wynn v. Francis, No. B245401, 2014 WL 2811692, at 3-4 (Cal. Ct. App. 2014).

[42.] Prinzing v. Schwab, No. A05–398, 2006 WL 538926, at *1 (Minn. Ct. App. Mar. 7, 2006).

and marriage, stating that "she was personally humiliated, and one of her children was taunted at school," forcing her to move to a different vicinity that was unaware of the case.[43] The jury awarded her $150,000 in damages as a result of her testimony. This case demonstrates how courts assess and compensate not only for damage to one's professional reputation but also for emotional harm resulting from defamation, regardless of one's social or economic status.

Victims often experience stress and anxiety, panic attacks, and depression. Other common problems include insomnia, eating disorders, alcohol and substance abuse, and in some cases, thoughts of self-harm or suicide. In proving emotional distress, reports from psychologists or psychiatrists help document mental issues. Other essentials include related medical records from doctors' visits and prescriptions to medications used to combat anxiety. More severe cases might result in ER visits or hospitalization. Victims may suffer panic attacks, strokes, or heart problems. In defamation cases, these issues are both documentable and compelling as evidence.

4. Rehabilitation Repair Damages

Victims can begin the process of repairing damages to their reputation by legally forcing the removal of defamatory content. However, defamation travels far and fast online, often causing irreversible harm before the victim can respond.[44] This viral nature of defamation in the digital age has necessitated awards for reputation rehabilitation costs, particularly for online defamation. Courts treat these as compensatory damages akin to medical treatment for physical harm.[45] Just as there are mechanics to fix your car, electricians to fix your lights, and surgeons to fix your hernia, there are reputation professionals and companies that specialize in helping restore a person's or company's reputation. One central strategy employed is the suppression of defamatory content online. These experts and companies identify the audience that was exposed to negative content and target it with new, positive content.

Complete removal of anything posted on the internet is also impossible in most cases. For example, despite Dominion Voting Systems' case against Fox News forcing retractions and settlements, Fox's original false claims proliferated online, with many users continuing to believe them long after the court's decision was rendered.[46] Users can take screenshots of posts before their removal, sharing them indefinitely after their deletion. Therefore, beyond forcing removal of content, victims can create new content narratives to replace the negative content. This strategy looks at search engine results pages (SERPs) and where defamatory statements appear in results. Publishing favorable content on trusted platforms can dilute negative search results. By creating and posting positive content on high-authority domains, burying negative content is possible, pushing it down to the fifth or sixth page of search results on the name of the individual or business in question.

Not surprisingly, this process is costly and time-consuming, and it requires a diverse range of expertise. The job is usually carried out by online reputation management companies that help individuals and organizations build and monitor brands and reputations and manage crises when they do arise. As seen in the aftermath of high-profile cases such as *Carroll v. Trump* and *Giuliani v. Freeman*, reputation professionals employ suppression strategies when removal is impossible.

[43.] Supra.

[44.] *See* Danielle Keats Citron, *Hate Crimes in Cyberspace*, 45 (2014).

[45.] *See Doe v. Ciolli*, 611 F. Supp. 2d 216, 221 (D. Conn. 2009).

[46] Patrick Marley and Jeremy Barr, *After Fox Settlement, Experts Warn Falsehoods Will Persist*, The Washington Post, (April 19, 2023).

In the first *Carroll v. Trump* case, the plaintiff's expert calculated that a rehabilitation campaign to try to restore the plaintiff's reputation might cost as much as $15 million.[47] Although courts in some jurisdictions consider the costs for these services to be speculative, many courts have acknowledged these efforts as legitimate, awarding damages to cover their costs if proven to mitigate measurable harm.[48]

Effective suppression can sometimes require six months to a year of sustained effort by firms with expertise in legal, PR, and SEO skills. A number of state courts have acknowledged this and approved expert testimony from reputation specialists.[49]

5. Loss of Reputation Damages

This last category is the most conceptually complex but often the most important component for plaintiffs. Unlike economic or emotional distress damages—which, though complex to calculate, are squarely quantifiable—damage to one's reputation can be proven through witness testimony or other corroborating evidence to demonstrate that the victim has experienced negative social repercussions as a result of defamation.

To illustrate this, let us first consider a hypothetical example. A 70-year-old retired man is defamed. He is falsely accused of committing a heinous crime, and the accusation spreads far and wide in the news and on social media before the truth emerges. Since he is retired, he does not have the same professional losses of income, employment, and future opportunities that working people would face. His social security check still comes, and his other retirement assets remain. Likewise, he did not suffer emotional damage, and at his age, launching a rehabilitation campaign does not make sense, so the first four types of damages do not apply. However, his reputation—the one he worked for decades to develop—is destroyed. It's the only reputation he has.

People in church no longer sit next to him. He is not invited to the neighborhood block parties. His neighbors don't shovel his driveway anymore in the winter. Obviously, his loss of reputation is harm in and of itself.

This last category is often the only category for defamation *per se* cases. In many jurisdictions, in the absence of concrete evidence, reputational harm can extend into the realm of presumed damages, allowing a plaintiff to recover damages to reputation without tangible proof of harm.[50] In assessing damages, as some have noted, the presumed damages rule "has had remarkable staying power in American law" in part because reputation acts as a vital social currency.[51]

Presumed damages were recognized by the U.S. Supreme Court in *Gertz v. Robert Welch, Inc*., mentioned earlier for its support for mental anguish damages.[52] In this case, the Court expressed the view that reputation is an important interest worthy of legal protection, one that reflects our basic concept of the essential dignity of people. However, modern courts have sought valuation methods that are more well-defined, particularly in jurisdictions that limit presumed

---

[47.] E. Jean Carroll v. Donald J. Trump, No. 23-1045, 2d Cir. (S.D.N.Y. 2023).

[48.] Robert D. Sack, *Sack on Defamation*, 4:3.2 (5th ed. 2023).

[49.] Ampex Corp. v. Cargle, 128 P.3d 996, 1003 (Okla. Civ. App. 2005).

[50.] Restatement (Second) of Torts § 621 cmt. a (Am. L. Inst. 1977).

[51.] Michael K. Steenson, *Presumed Damages in Defamation Law*, William Mitchell Law Review, Vol. 40, Issue 4, 1491 (2014).

[52.] Gertz v. Robert Welch, Inc. 418 U.S. 323, 350 (1974).

damages. This was expressed in *New York Times v. Sullivan where* the court found that to sustain a claim of defamation or libel, the First Amendment requires that the plaintiff show that the defendant knew that a statement was false or that the defendant was reckless in deciding to publish the information without confirming that it was accurate.[53] In the case of *Wynn v. Francis*, the jury awarded the plaintiff $17 million for presumed damages to his reputation.[54] The size of the award demonstrates how seriously many courts take defamation that results in negative consequences on a person's career or professional reputation.

Reputational damages can also occur in cases involving corporations. In *Brown & Williamson Tobacco Corp. v. Jacobson* (1987), the plaintiff successfully proved that a television broadcast had falsely accused the tobacco company of intentionally advertising to minors.[55] Despite being unable to prove any economic loss caused by the defamation, the jury awarded $3 million in presumed damages to the Plaintiffs.[56]

Many jurisdictions impose a presumed damages rule because of "the overriding state interest in protecting reputation and the difficulty—if not the impossibility—of providing evidence of actual injury to reputation."[57] This allows juries to assign a value to reputational harm independent of its direct economic or physical impacts. Although most states hold that damage is implied in *per se* cases, eight states have eliminated presumed damages as unconstitutional, often citing *Gertz v. Welch* (This landmark case, cited earlier for its impact on emotional distress damages, also set important precedent with respect to Constitutional versus state law).[58] Other states have placed special restrictions on damages in per se cases.[59] For example, Iowa has excluded libel *per se* and presumed damages in defamation cases involving media defendants.[60]

Although there remains no easy answer to the ideal way of quantifying a victim's loss of reputation, as with other aspects of defamation damages, finding a value often involves nuances that expert witnesses help explain. Below are useful constructs that can provide a degree of clarity in breaking down the sub-elements that contribute to an overall loss of reputation.

III. THE THREE RINGS OF REPUTATIONAL DAMAGE

Given the elusive conceptual nature of reputation, it becomes useful to consider the various layers of relationships that determine one's social standing. Legal scholars have rightly noted that reputation is "not a monolith but a network of perceptions held by different communities."[61] As such, when assessing damages, courts consider the different levels of personal and professional associations that people maintain and how each group is variously affected by the defamation in question. Although not strictly legal terminology, these "rings of relationships" help outline the

---

[53.] N.Y. Times Co. v. Sullivan, 376 U.S. 254, 267 (1964).

[54.] Wynn v. Francis, No. B245401, 2014 WL 2811692, at 3-4 (Cal. Ct. App. 2014).

[55.] Brown & Williamson Tobacco Corp. v. Jacobson, 713 F.2d 262, 9 Media L. Rep. 1936 (7th Cir. Ill. July 14, 1983).

[56.] Supra.

[57.] NYT v. Sullivan at 1521.

[58] The court in *Gertz v. Welch* found that that liability in defamation cases against individuals cannot be imposed without fault, but states otherwise can craft their own defamation laws. However, plaintiffs are limited to actual damages if the state does not require actual malice to be shown.

[59.] Susan E. Seager, *Jackpot! Presumed Damages Gone Wild—and Unconstitutional*, Communications Lawyer, Vol. 3, Issue 1 (2015).

[60.] Beirman v. Weier, 826 N.W.2d 436, 447 (Iowa 2013).

[61.] Daniel J. Solove, The Future of Reputation: Gossip, Rumor, and Privacy on the Internet, Yale University Press, 51 (2007).

scale of reputational damages, particularly as it is the hardest type of damage to calculate. In my work as an expert witness, I have used this theory to estimate damages, and my findings have helped calculate reputational damages and assist legal teams in settlements.

Within this metaphor, the three rings consist of:

A. Ring 1. The Inner Ring (Family, Close Friends, and Intimate Associates)

This is the "inner ring," consisting of those closest to the defamation victim, including family, near friends, and close co-workers. This is the most damaging ring emotionally, when the people most cherished by the victim hear the false accusations. Because false accusations can splinter deeply personal bonds, this ring often causes emotional and mental distress. Courts have established that defamation can cause "mental anguish, humiliation, and damage to familial relationships."[62] In fact, loss of social connections and being cut off from one's immediate community are central to the concept of reputational damage, and being isolated from community activities can decrease a person's mental health.[63] In expert witness calculations, the damage to this ring may be calculated by direct interviews and quotes with relevant individuals to ascertain their perception and observation of any changes in or for the concerned person.

However, this ring is also the easiest to manage since the victim can speak to this group directly, and they may be disposed to disbelieve rumors about a person they know. Studies from psychologists indicate that close personal relationships are better able to resist outside threats, given the pre-existing trust that exists between two people with familial or fraternal ties. So, while the harm is significant and at times the most damaging, it is likely the easiest to remedy.

B. Ring 2. The Middle Ring (Acquaintances, Colleagues, and Social Networks)

The "middle ring" consists of acquaintances, lesser friends, neighbors, fellow churchgoers, former schoolmates, and coworkers. These are people who know the victim, but not well. They perhaps see the person only occasionally. For this middle ring, the harm is acute since all these individuals know and recognize the victim, but usually not well enough that they will approach the person and ask whether the accusations were true. In fact, often this group will avoid the victim and the awkwardness that bringing up such rumors would entail. Typically, however, they won't avoid broaching the subject among one another. Instead, they may avoid the victim to skirt uneasiness while still gossiping about the allegations among themselves, a phenomenon of rumor spreading scholars have called "social cascades."[64]

The damage here may again be calculated through direct or indirect experiential interviews, any evidence of social change towards the plaintiff, documentation of lost opportunities, or questions being asked about the plaintiff from the inner circle.

This group weighs heavily on the victim's social status and daily activities, as they form the foundation of a victim's social and professional network. They can also impact job mobility, since most job referrals and opportunities derive from one's network of acquaintances, which includes this middle ring. Defamation within this ring can thus devastate career prospects, as seen in cases where professionals lost business partnerships due to false accusations.

---

62. Gertz v. Robert Welch, 418 U.S. 323, 347 (1974).

63. See Robert D. Putnam, Bowling Alone: the Collapse and Revival of American Community, Touchstone Books/Simon & Schuster (2000).

64. Cass R. Sunstein, On Rumors: How Falsehoods Spread, Why We Believe Them, and What Can Be Done (2009).

C. Ring 3. The Outer Ring (The General Public and Strangers)

This "outer ring" consists mostly of strangers. These are outsiders who have never met the defamation victim or possibly even heard the victim's name previously. On one hand, the damage for this outer ring seems negligible, since these are strangers, not people the victim will likely have to face. On the other hand, this is a nearly infinite group that knows the wrongfully accused person only by the false accusations, with many people disposed to assume accusations are true unless they hear otherwise. The victim will always know this group is out there, and that someone from this group may be the next personnel manager of a potential client the victim hopes to impress.

In extreme cases of defamation, victims and their families are forced to move to a different geographic location to avoid stigma. In a new location, where their names and faces are lesser known, they may be able to continue in their occupations, begin new ones, or just lead normal lives. But even after moving, the victims and their families know that over the internet, their damaged reputations may follow them through Google searches and other means, whether ahead of a job interview or by curious classmates.[65]

If we look again at the recent high-profile cases, we see how this third ring can be devastating. Politicians, celebrities, and authors rely on public perception—meaning defamation can destroy careers. For politicians, the ring includes voters; for authors like E. Jean Carroll, readers; and for actors like Johnny Depp and Amber Heard, the moviegoers whose admiration can make or break Hollywood careers. This layer of complexity elevates celebrity defamation cases to another level, in both the complexity of the cases and the size of the monetary damages. Mass-media defamation, in fact, can lead to multimillion-dollar verdicts.

In recent cases, I have calculated damages from harm to the third ring by calculating the precise number of a celebrity's fans who saw the damaging narrative online and/or in stores and assigned dollar values to these numbers to calculate a range of damages based on reputational harm.

IV. UNSETTLING VERDICTS

Especially in high-profile cases, even detailed documentation of various damages and the most skilled expert witness testimony does not erase the ambiguity. Court rulings are often appealed, and settlement negotiations lead in numerous directions. Moreover, gaining a favorable judgment and actually receiving the damages owed are not the same.

In the Rudy Giuliani case, the two Georgia election workers sued, saying Giuliani's false claims of election fraud had upended their lives by inciting racist threats and harassment—misinformation that Giuliani refused to stop repeating. Their stories were compelling. As the Associated Press reported, following emotional testimony, there was "an audible gasp" in the courtroom when the jury's foreperson read aloud the award of $75 million in punitive damages, added to $36 million each in other damages.[66] Still, eight months later they were back in court asking a federal court to help enforce the judgment, listing the assets of the former New York mayor, including properties in New York and Florida, a Mercedes-Benz, some two-dozen luxury watches, sports memorabilia including three New York Yankees World Series rings, and other personal items.

[65.] Prinzing v. Schwab, No. A05–398, 2006 WL 538926, at *1 (Minn. Ct. App. Mar. 7, 2006).

[66.] Lindsay Whitehurst and Alann Durkin Richer, *Jury Awards $148 Million in Damages to Georgia Election Workers*, AP News (Dec. 15 2023).

In the case of Alex Jones, who claimed the 2012 Sandy Hook school shooting that killed 20 children and six adults was a hoax staged by actors, he was found guilty of libel by a Connecticut jury for nearly $1 billion, and a month later, an additional $473 million in punitive damages. In a separate case in Texas, Jones was ordered to pay $49 million in damages to Sandy Hook parents, $4.1 million of that in compensatory damages and $45.2 million in punitive damages. But how much of those damages the plaintiffs will ever receive remains uncertain. Jones's Infowars media business was set to be auctioned off in October 2024 as part of bankruptcy proceedings.[67]

The eye-popping $787.5 million settlement in Dominion's case against Fox News came with an added layer of complexity. The trial was scheduled to begin in April 2023, with Dominion planning to subpoena Fox Corp. Chairman Rupert Murdoch and his son, Fox Corp. CEO Lachlan Murdoch. Fox News hosts, including Sean Hannity and Tucker Carlson, were also likely to be called for testimony. Fox News had already been subjected to months of negative publicity, and the prospect of a trial apparently induced the company to accept the gigantic settlement.

The Fox Corp. suit is one of several cases related to false claims of voter fraud. The voting tech company Smartmatic reached a "confidential settlement" on Sept. 26 with Newsmax, another right-leaning cable channel, and a similar settlement in April with One America News, and the company is still involved in a lawsuit against Fox News.[68] The political sensitivity of these cases, involving false claims of voter fraud, cannot be overstated, given their impact on public trust in the democratic process.

Finally, the Johnny Depp–Amber Heard case shows clear examples of how calculating defamation damages is often far from an exact science. Originally, Depp sued Heard for defamation, claiming $50 million in damages, and Heard filed a countersuit claiming $100 million in damages. In its finding, the jury awarded Depp with $10 million in compensatory damages and another $5 million in punitive damages. The punitive damages, however, were reduced to $350,000 because of limits imposed by Virginia state law—the trial was held in Fairfax County, Virginia. Less reported is the award in Heard's countersuit. The jury found that a contested statement made by Depp's lawyer to be false and defamatory and awarded Heard $2 million in compensatory damages.

Both sides appealed the judgments against them in late 2022 and, in December, settled the case and dropped their appeals. Many commentators noted Depp had won the closely followed case in the court of public opinion, and as for the damages, Depp's attorney stated that the "jury's unanimous decision and the resulting judgment in Mr. Depp's favor against Ms. Heard remain fully in place," and the settlement would result in a $1 million payment to Depp—paid by Heard's homeowner's insurance—which "Depp is pledging and will donate to charities."[69]

Thus are the complexities of defamation damages from original calculations and documentation through court proceedings and actual payment. From Trump to Giuliani, from Dominion to Depp, significant efforts that factor into the assessment of damages reflect society's broader struggle to value reputation in the digital age. As both state and federal courts have recognized, the future lies in evidence-based frameworks that account for how harm spreads online, including not only the falsehood of the defamatory statements or the malicious intent

---

[67.] Akiko Matsuda, Infowars for Sale: Alex Jones's Assets Again Debated in Bankruptcy Court, Wall Street Journal (Sept. 19 2024).

[68.] Sara Fischer, Newsmax, Smartmatic Settle Defamation Lawsuit, Axios (Sept. 27, 2024).

[69.] Elyse Dupre, Johnny Depp to Donate $1 million Settlement from Amber Heard to 5 Charities, NBC Los Angeles (2023).

behind them, but also the speed at which they travel and the extent of their geographic reach in determining the effects of their reputational harm.

DEFINING THE LEGAL GUARDRAILS: AN ANALYSIS OF ACCEPTABLE USE POLICIES FOR AI TECHNOLOGIES

SUVRANGSHU SEN[*]
JOEY ROBERTSON[**]
ASHLY BENDER SMITH[***]
DIANA BROWN[****]

I. INTRODUCTION

Artificial intelligence (AI) can be thought of as computerized systems that work and react in ways commonly considered to require human intelligence, such as learning, solving problems, and achieving goals under uncertain and varying conditions, with varying levels of autonomy.[1] AI can encompass a range of technologies, methodologies, and application areas, such as natural language processing, robotics, and facial recognition.[2]

Generative AI refers to artificial intelligence that can create new content—such as text, images, music, code, or video—by generating data similar to its training set. These models learn patterns and structures from existing data and use them to produce original outputs in response to prompts.[3] Generative AI models do not "store" copies of images, text passages, or music files in the way a hard drive does; instead, the models store numerical parameters that represent learned statistical patterns and relationships derived from the training data.[4] When generating output, the model uses these parameters to synthesize new data points within the learned distribution; the process is one of synthesis and statistical inference based on learned patterns, not retrieval of stored originals.[5]

Generative AI tools based on large language models, like ChatGPT, Claude, and Microsoft CoPilot are rapidly gaining acceptance throughout the world.[6] Organizations of all sizes and across nearly all industries recognize the transformative power of generative AI tools.[7] While many

---

[*] M.B.A. Candidate, Sam Houston State University
[**] J.D., Professor, Sam Houston State University
[***] Ph.D., Associate Professor, Sam Houston State University
[****] J.D., Associate Professor, Sam Houston State University

[1] Congressional Research Serv., *Generative Artificial Intelligence: Overview, Issues, and Considerations for Congress*, CRS In Focus, IF12426 (Apr. 2, 2025), www.congress.gov/crs-product/IF12426.

[2] *Id.*

[3] *What Is Generative AI?,* CALIFORNIA INSTITUTE OF TECHNOLOGY, scienceexchange.caltech.edu/topics/artificial-intelligence-research/generative-ai.

[4] Jordi Linares-Pellicer *et al.*, *We Are All Creators: Generative AI, Collective Knowledge, and the Path Towards Human-AI Synergy*, CORNELL UNIVERSITY ARXIV (April 10, 2025), arxiv.org/html/2504.07936v1#:~:text=Generative% 20AI%20models%20do%20not,distinct%20form%20of%20alternative%20intelligence.

[5] *Id.*

[6] Alexander Bick, Adam Blandin, and David J. Deming, *The Rapid Adoption of Generative AI*, CT STATE (Sept. 18, 2024), ctstate.edu/images/Forms-Documents/AI-presidential-fellows/The-Rapid-Adoption-of-Generative-AI.pdf.

[7] *Id.*

individuals are familiar with the publicly available versions of the tools, many large companies, and in some cases smaller companies, have in-house, proprietary generative AI tools.[8] Organizations and individuals use these tools to shorten research time, make predictions, summarize large data sets, draft reports and correspondence, write computer code, summarize meetings, create presentations and images, and more.

Agentic AI tools, on the other hand, are designed to autonomously make decisions and act to achieve complex goals with minimal human supervision.[9] These tools combine large language models (LLMs), machine learning (ML), reinforcement learning, and natural language processing (NLP) to operate independently and adapt to changing situations.[10] Autonomous driving is an example of Agentic AI.[11] Both Generative AI and Agentic AI fall under the broader umbrella of advanced artificial intelligence technologies.[12]

Properly integrated into workflows and used with clear purpose, AI tools can unlock remarkable gains in productivity.[13] However, these tools may also generate flawed outputs, stemming from coding errors, inherent biases, or deficiencies in their training data.[14] Therefore, sources of unintended outcomes can reside within the model's design and training long before any user interaction. In addition, these tools can be used unethically, such as utilizing training datasets that favor one demographic while deliberately excluding others.[15]

Due to these concerns and others, companies that create and/or use generative AI tools write policies that guide individuals' use of the tools, including requiring individuals to use the tools responsibly and with awareness of potential risks.[16] These policies can broadly be referred to as "Acceptable Use Policies," and this term is used with regard to both tools and products.[17]

This paper examines the principles and best practices underlying acceptable AI use policies within organizational settings by analyzing current events, high-profile cases, emerging litigation trends, and other legal considerations related to artificial intelligence. The objective is to evaluate whether a comprehensive acceptable use policy can serve as an effective safeguard and risk management tool for companies against potential legal and reputational liabilities stemming from AI misuse. The paper provides practical insights and recommendations for organizations seeking

---

[8] Joaquin Fernandez, *The Leading Generative AI Companies*, IoT ANALYTICS (Mar. 4, 2025), iot-analytics.com/leading-generative-ai-companies/.

[9] Teaganne Finn and Amanda Downie, *Agentic AI vs. Generative AI,* IBM, www.ibm.com/think/topics /agentic-ai-vs-generative-ai.

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] See, *e.g.,* Aaron Mok, *Leaders at PwC, Mastercard, IKEA, and More Who Are Driving AI Adoption*, BUS. INSIDER (Jun 10, 2025, 1:50 PM), //www.businessinsider.com/ai-leaders-pwc-mastercard-accenture-ikea-tech-adoption-growth-strategy-2025-5; Hsing Tseng*, How to Use ChatGPT for Brainstorming,* WASH. POST (Dec. 2, 2024), zapier.com/blog/chatgpt-for-brainstorming/; Thomas Dohmke, Marco Iansiti & Greg Richards, *Sea Change in Software Development: Economic and Productivity Analysis of the AI-Powered Developer Lifecycle*, CORNELL UNIVERSITY ARXIV (June 26, 2023), arxiv.org/abs/2306.15033.

[14] Generative AI Working Group, *When AI Gets It Wrong: Addressing AI Hallucinations and Bias*, MIT MANAGEMENT, mitsloanedtech.mit.edu/ai/basics/addressing-ai-hallucinations-and-bias/.

[15] Thomas Dethmann and Jannis Spiekermann, *Ethical Use of Training Data: Ensuring Fairness and Data Protection in AI, LAMARR INST.* (July 3, 2024), lamarr-institute.org/blog/ai-training-data-bias/.

[16] Diana Leiden and Helen Winters, *Harnessing Generative AI: Best Practices for Trade Secret Protection*, WINSTON & STRAWN (June 26, 2024), www.winston.com/en/insights-news/harnessing-generative-ai-best-practices-for-trade-secret-protection.

[17] Richard Bevis, *What Is an Acceptable Use Policy?*, CBT NUGGETS (Oct. 11, 2024), www.cbtnuggets.com/blog/technology/data/what-is-acceptable-use-policy.

to implement robust AI governance frameworks that balance innovation with accountability and risk management.

II. BACKGROUND

A. The Role of Acceptable Use Policies

Acceptable Use Policies (AUPs) are formal rules created by organizations to outline how their technology resources (products or services) are to be used responsibly, as well as how the products or services should not be used.[18] AUPs can be inward-facing or outward-facing. An inward-facing AI AUP provides guidelines for an organization's employees, contractors, and internal teams on the responsible and secure use of AI technologies in the workplace.[19] An outward-facing AI AUP governs how other stakeholders such as external customers, collaborators, and developers, as well as the general public, interact with an organization's publicly available AI systems or services (*e.g.*, an AI-powered chatbot on a website, or a public Application Programming Interface (API)).[20]

An AUP is important because, without a defined policy, employees are left guessing what is safe, or even worse, not considering the issue of safety at all.[21] Additionally, when teams experiment with AI without a defined policy, "Shadow AI" can infiltrate the organization.[22] "Shadow AI" refers to the use of artificial intelligence tools or models without Information Technology (IT) security oversight.[23] The use of unsanctioned AI tools, models, or services by employees (or third parties, including vendors or service providers) without formal approval, oversight, or integration into the enterprise's governance, security, and data controls is problematic.[24] Because AI tools can ingest or generate sensitive content, interact with APIs, and propagate errors or vulnerabilities at scale, the absence of a clear Acceptable Use Policy (AUP) exposes the organization to data breaches, compliance violations, and operational risks that can undermine trust and security. For instance, seemingly innocent usage of AI often includes problematic incidents such as an employee pasting customer data into ChatGPT to summarize it; the marketing department using an unvetted AI image generator that violates copyright; engineers using unvetted open-source models to cut costs on a proof of concept; a developer uploading source code for debugging help; customer service representatives asking ChatGPT for help drafting an email; a finance team member using a forecasting tool after feeding it internal budget

---

[18] *Id.*

[19] Ashley Lejserowits, *AI Acceptable Use Policy: What It Is, Why It Matters, and How to Create One*, PROMPT SECURITY BLOG (Oct. 9, 2025), prompt.security/blog/ai-acceptable-use-policy-what-it-is-why-it-matters-and-how-to-create-one.

[20] Bevis, *supra* note 17. An Application Programming Interface (API) is a set of rules, protocols, and tools that allows different software applications to communicate and exchange data or without needing to know each other's internal code, enabling features like weather updates in apps, single sign-on, and payment processing. APIs simplify integration, automate processes, and allow developers to leverage existing services, fostering the creation of interconnected digital systems. *See,* MULESOFT, www.mulesoft.com/api/what-is-an-api.

[21] *Id.*

[22] *Id.*

[23] Bryan Arnott, *What is Shadow AI and How to Stop It*, FORCEPOINT (October 23, 2025), www.forcepoint.com/blog/insights/what-is-shadow-ai.

[24] Matthew White *et al*, *Cybersecurity Awareness Month 2025: Don't Get Haunted by Shadow AI,* BAKER DONELSON (October 21, 2025), www.bakerdonelson.com/cybersecurity-awareness-month-2025-dont-get-haunted-by-shadow-ai#:~:text=What%20Lurks%20in%20the%20Shadows,errors%20or%20vulnerabilities%20at%20scale.

spreadsheets; or salesmen recording a strategic sales meeting with an AI application to summarize action items.[25]

This unmonitored AI use can inadvertently expose confidential information, proprietary designs, customer data, trade secrets, and other intellectual property to external systems and public models beyond organizational control that retain and reuse input data.[26] Additionally, unmonitored AI use may produce biased or inaccurate outputs, harming brand credibility and/or misleading customers.[27] Further, in regulated industries, these failures can lead to compliance violations, regulatory penalties, and reputational damage that far exceed any short-term productivity gains.[28]

These policies not only govern employees' interactions with AI technology but also extend beyond mere usage guidelines to encompass broader organizational and ethical considerations.[29] It is essential to account for the potential internal and external use or integration of any generated output.[30] Responsibility for the downstream consequences of questionable or flawed output may flow through the entire chain of utilization, beginning with the creator.[31]

This problematic usage or output often proliferates in downstream use, integration or application, and is caused when the original creator fails to understand the limitations of the tool.[32] AUPs, with careful drafting and proper adherence and enforcement, can limit the number of issues, and thereby limit legal liabilities, resulting from such problematic usage.[33]

B. Inherent Concerns with Generative/Agentic AI

Generative and agentic AI tools can be inherently flawed. Generative AI models consist of billions of interconnected parameters functioning analogously to neurons in the human brain, collectively producing responses based on pre-existing data.[34] Each parameter is assigned a weight, which is optimized during training through exposure to vast datasets comprising billions of examples.[35] The interaction among these weights is critical for generating accurate outputs from a given input.[36] Notably, variations in weight configurations can lead to substantially different outcomes, even when the input data remains unchanged.[37]

Even when generative or agentic AI systems exhibit minimal inherent bias or error, these systems remain fundamentally non-sentient and cannot explain the reasoning behind their

---

[25] *Id.*; See also, Lejserowits, *supra* note 19; White, *supra* note 24.
[26] *Id*.
[27] Lejserowits, *supra* note 19.
[28] *Id.*
[29] *Id.*
[30] Bevis, *supra* note 17.
[31] *Id.*
[32] Haoyu Gao *et al*., *AI Safety in the Eyes of the Downstream Developer: A First Look at Concerns, Practices, and Challenges*, CORNELL UNIVERSITY ARXIV (Mar. 25, 2025), arxiv.org/html/2503.19444v1.
[33] Bevis, *supra* note 17.
[34] Edmund T Rolls, *The Memory Systems Of The Human Brain And Generative Artificial Intelligence*, NATIONAL INSTITUTE OF HEALTH (May 24, 2024), pmc.ncbi.nlm.nih.gov/articles/PMC11152951/#:~:text=2., available%20%5B10%2C12%5D.
[35] Cole Stryker and Mark Scapicchio, *What Is Generative AI?*, IBM THINK (2024), www.ibm.com/think/topics/generative-ai.
[36] Willians Ericson, *Unveiling the Core: A Deep Dive into Neural Networks, Weights, and the Future of AI*, MEDIUM (Jan. 15, 2025), medium.com/@ericson_willians/unveiling-the-core-a-deep-dive-into-neural-networks-weights-and-the-future-of-ai-aa75705d038e.
[37] *Id.*

outputs.[38] Each response reflects a context-specific interpretation of the user's input at that point in time.[39] Because user inputs may introduce intentional or unintentional biases, inaccuracies, or other flaws, the risk of unethical application persists.[40] In business settings, a common issue arises when employees overlook the intrinsic limitations of these tools.

Such limitations include the model's inability to perform well on tasks that are dissimilar to the examples it encountered during training, which restricts the model's ability to generalize and adapt effectively to new or changing contexts.[41] Generally speaking, AI is highly effective at recognizing patterns and generating outputs based on the distribution of data upon which it was trained.[42] However, this strength is also a limitation: when faced with new, out-of-distribution, or contextually different inputs, the model may struggle because it lacks true adaptability or reasoning beyond learned patterns.[43] An easy to understand example of this concept is described by Gary Marcus: "…I once trained an older [LLM] model to solve a very basic mathematical equation using only even-numbered training data. The model was able to generalise [sic] a little bit: solve for even numbers it hadn't seen before, but unable to do so for problems where the answer was an odd number."[44] This problem remains unsolved: "More than a quarter of a century later, when a task is close to the training data, these systems work pretty well. But as they stray further away from that data, they often break down."[45]

Given these concerns, blind reliance on outputs from generative or agentic AI systems can pose significant enterprise risks. Such risks include the propagation of misinformation when outputs contain factual inaccuracies, the amplification of biases embedded in training data or user inputs, and the inadvertent disclosure of sensitive information through poorly managed prompts.[46] Additionally, outputs can create ethical and legal challenges, such as intellectual property violations or discriminatory content, which can lead to reputational harm and regulatory non-compliance.[47]

These vulnerabilities underscore the necessity of human oversight and critical evaluation when integrating AI-generated content into the decision-making processes of any business enterprise. Human oversight is largely achieved through "human-in-the-loop" (HITL) systems, which integrate human judgment, context, and ethics into AI processes for review, correction, and ultimate decision-making, ensuring systems remain reliable, fair, and aligned with human values, especially in regulated industries where full automation is not desirable or safe.[48] It is best thought of as a collaborative partnership, not just a safety net, involving humans providing feedback during training or intervening in real-time operations, reconciling between AI's speed and scale with

---

[38] Linares-Pellicer, *supra* note 4; Rolls, *supra* note 34.
[39] *Id.*
[40] *Id.*
[41] Gary Marcus, *When Billion-Dollar AIs Break Down Over Puzzles A Child Can Do, It's Time To Rethink The Hype*, THE GUARDIAN (June 10, 2025), www.iask.ca/news/2afca18bec3c9cda2346c2138205625e.
[42] *Id.*
[43] *Id.*
[44] *Id.*
[45] *Id.*
[46] Lubov McKone, *Bias in AI: How to Spot It, Why It Matters, and What You Can Do*, JOHNS HOPKINS UNIVERSITY (Sept. 29, 2025), www.library.jhu.edu/bias-in-ai-how-to-spot-it-why-it-matters-and-what-you-can-do/.
[47] Lejserowits, *supra* note 19.
[48] John Brewer, *Human in the Loop: A Necessity for Using AI Tools*, THE CLOUD AWARDS (November 18, 2024), www.cloud-awards.com/human-in-the-loop-necessity-for-using-ai#:~:text=Yet%2C%20as%20powerful%20as%20AI,harness%20AI%20responsibly%20and%20effectively.

human nuance and ethics.[49] No AI system, no matter how sophisticated, is foolproof.[50] Human intervention for oversight, validation and refinement is not just a safeguard but an integral part of ensuring accuracy, fairness, and accountability in AI systems.[51]

III. Analysis of Risks Identified in Ten Organizations' Acceptable AI Use Policies

For this study, the acceptable AI use policies of ten large organizations were analyzed to identify which risks the organizations recognize when providing guidance to their employees and/or product users. These policies provide insight into the current state of corporate governance around AI adoption and highlight gaps that may expose organizations to operational, legal, and reputational risks.

A. Organization and Policy Selection

Because larger organizations are more likely to have the prominence to shape industry behavior, the ten companies included in this study all have at least fifty thousand employees and a revenue in the tens of billions of dollars (or euros). Broadly, the organizations included in this study sell their customers either products (including software systems) or consulting services. Each of these companies also has specific AI programs that are used by their employees or customers. Given their scale and deep involvement in generative AI development and/or use, these companies are likely to adopt innovative approaches when drafting AUPs. The extensive stakeholder networks and diverse employee roles in these organizations, combined with significant reputational and financial exposure, create strong incentives for comprehensive governance frameworks.

Given the size and revenue of these companies, it is also likely the organizations include sophisticated legal departments (or in the alternative, utilize specialized outside counsel) who play a crucial role in developing and implementing their AI policies. These attorneys are responsible for navigating the complex and evolving landscape of AI-adjacent law, including intellectual property rights, data privacy regulations, compliance issues, and liability concerns. Their involvement ensures that AI usage adheres to applicable laws and mitigates potential legal risks. This legal oversight must balance agile innovation with the need for robust compliance and risk management.

Finally, each organization's policy is publicly available and was authored in or after 2022. Both customer-facing (external) and employee-facing (internal) documents were analyzed. Some of the AUPs, notably including that of Salesforce, specify conditions under which AI usage constitutes a violation and delineates what behaviors are considered unacceptable. For many others, however, the guidelines are more general in nature and encompass partners, employees, and customers within their scope.

Table 1 provides an overview of the selected organizations and their AUP frameworks. The companies fall into two primary categories: technology providers (*e.g.,* Amazon, Meta, Microsoft, Google, IBM, Salesforce) and consulting firms (*e.g.*, KPMG, Ernst & Young, Deloitte, McKinsey). Technology companies primarily target internal audiences with their policies, reflecting governance over employee use of AI tools within product development and operations. In contrast,

[49] *Id.*
[50] *Id.*
[51] *Id.*

consulting firms focus on external audiences, emphasizing client-facing guidelines for responsible AI integration. The organizations vary significantly in size and revenue—from McKinsey's 45,100 employees and $16 billion revenue to Amazon's 1.56 million employees and $574.8 billion revenue—highlighting the diverse scale and influence of these entities in shaping AI governance practices. A review of each company's AUP provides insight into how industry leaders are identifying and addressing the potential risks of generative AI tools.

Table 1. Summary of Included Organizations and their Policies

Company	**Primary Offering**	**NAICS code**	**No. of Employees**	**Revenue**	**Policy Audience**
Amazon[52]	Products/Systems	454110, 518210	1,556,000	$574.8B	Internal
Meta[53]	Products/Systems	519130	74,067	$116.61B	Internal
Microsoft[54]	Products/Systems	511210, 518210	228,000	$198.27B	Internal
Google[55]	Products/Systems	519130	190,234	$282.84B	Internal
IBM[56]	Products/Systems	518210, 511210	303,100	$60.53B	Internal[57]
KPMG[58]	Consulting	541211, 541219	275,288	€36.576B (~$39.3B)	External
Ernst & Young[59]	Consulting	541211, 541219	500,000 (projected)	Not disclosed	External
Deloitte[60]	Consulting	541211, 541219	457,000	$64.9B	External
McKinsey[61]	Consulting	541611, 541618	45,100	$16B	External
Salesforce[62]	Products/Systems	511210, 518210	76,453	$37.895B	External

[52] Amazon Web Services, Inc., *Amazon Nova Acceptable Use Policy* (2025), docs.aws.amazon.com/nova/latest/userguide/responsible-use.html.
[53]Meta, *Meta AI's Terms of Service* (2025), www.facebook.com/legal/ai-terms.
[54]Microsoft, *Microsoft Enterprise AI Services Code of Conduct* (2025), learn.microsoft.com/en-us/legal/ai-code-of-conduct.
[55] Google, *Generative AI Prohibitive Use Policy* (2024), policies.google.com/terms/generative-ai/use-policy.
[56] Robert Hagemann & Jean-Marc Leclerc, *Precision Regulation for Artificial Intelligence,* IBM POLICY LAB (2020), www.ibm.com/policy/ai-precision-regulation/.
[57] IBM's policy is primarily for internal users but also applies to external users.
[58] Daniel Besch, Sebastian Demty & David Hajovsky, *AI and Automation in Financial Reporting,* KPMG LLP (2024), kpmg.com/us/en/frv/reference-library/2024/guide-ai-and-automation-in-financial-reporting.html.
[59] Nicola Morini Bianzino et al., *The Artificial Intelligence (AI) Global Regulatory Landscape,* ERNST & YOUNG (2023), www.ey.com/content/dam/ey-unified-site/ey-com/en-gl/insights/ai/documents/ey-the-artificial-intelligence-ai-global-regulatory-landscape-final.pdf.
[60] DELOITTE AI INSTITUTE, Proactive Risk Management in Generative AI (2025), www2.deloitte.com/us/en/pages/consulting/articles/responsible-use-of-generative-ai.html.
[61] Oliver Bevan et al., *Implementing Generative AI with Speed and Safety,* MCKINSEY & CO. (2025), www.mckinsey.com/capabilities/risk-and-resilience/our-insights/implementing-generative-ai-with-speed-and-safety.
[62] *Artificial Intelligence Acceptable Use Policy,* SALESFORCE (2024), www.salesforce.com/content/dam/web/en_us/; www/documents/legal/Agreements/policies/ai-acceptable-use-policy.pdf.

B. Regulatory Landscape

Although there is a growing consensus among governmental bodies regarding the potential risks and societal implications posed by generative AI technologies, the advanced AI sector remains largely unregulated. The Organization for Economic Cooperation and Development (OECD)[63] and Group of 20 (G20)[64] have broad guidelines in place. The OECD AI Guidelines, adopted in 2019 and updated in 2024, are a global standard promoting responsible AI, focusing on five principles for AI systems (inclusive growth, human rights/fairness, transparency, robustness, accountability) and five policy recommendations for governments (R&D investment, supportive ecosystems, enabling policies, workforce training, international cooperation) with the aim of fostering trustworthy AI that benefits society while mitigating risks like bias and privacy issues.[65] The G20 AI guidelines focus on making AI inclusive, human-centered, transparent, robust, and accountable, by promoting inclusive growth and sustainable development while respecting human rights, fairness, and the rule of law.[66] Key themes include building trust through transparency, ensuring safety and security, and establishing accountability for AI systems, while also encouraging investment in open, trustworthy AI systems, data sharing, and addressing societal impacts like job displacement and misinformation.[67]

The E.U. AI Act is the world's first comprehensive law for Artificial Intelligence, using a risk-based approach to regulate AI systems in four tiers: banning unacceptable risks (like social scoring), heavily regulating high-risk applications (*e.g.,* in hiring, critical infrastructure, law enforcement and border control, banking and insurance, education, and applications that determine the outcome of democratic processes), requiring transparency for limited-risk AI (including chatbots), and leaving minimal-risk systems (like video games and spam filters) largely unrestricted.[68] It aims to ensure AI is safe, ethical, and respects fundamental rights, imposing strict rules, quality data standards, and human oversight for high-risk systems.[69] The Act focuses on protecting dignity, freedom, equality, and justice, ensuring AI does not violate these fundamental rights.[70] The penalties that will apply under the AIA are expected to be very significant, ranging from €7.5 million (or 1.5% global annual turnover) to €35 million (or 7% global annual turnover) for the preceding financial year, depending on the type of infringement and the size of the company, with an AI Office to oversee implementation.[71]

The U.S. does not have a single overarching AI regulation equivalent to the E.U. AI Act. Instead, governance relies largely on executive orders and agency guidance. The United States has, of late, rescinded the guidelines that had been in place.[72] Executive Order 14110 (signed by President Biden in October, 2023) focused on the safe, secure, and trustworthy development and use of AI.[73] It required federal agencies to adopt risk management practices, transparency measures, and even mandated private companies to share results of safety tests for high-risk AI models.[74] However, on January 20, 2025, President Trump revoked Executive Order 14110 as part of a broader rescission of Biden-era executive orders. This was done through an order titled "Initial Rescissions of Harmful Executive Orders and Actions."[75]

---

[63] The OECD is an intergovernmental organization with 38 member countries, founded in 1961 to stimulate economic progress and world trade. www.state.gov/the-organization-for-economic-co-operation-and-development-oecd.

[64] The G20 is an intergovernmental forum comprising 19 sovereign countries, the European Union (EU), and the African Union (AU). The G20 has an annual meeting that is a forum where the leaders of the world's largest economies gather to discuss and coordinate policies on the most pressing global issues. www.dfat.gov.au/trade/organisations/g20.

[65] OECD, *AI Principles,* www.oecd.org/en/topics/sub-issues/ai-principles.html.

President Trump then issued Executive Order 14179 on January 23, 2025.[76] Titled "Removing Barriers to American Leadership in AI," the order focuses on promoting innovation and reducing regulatory burdens rather than imposing safety rules.[77] In essence, EO 14179 is a major policy shift to deregulate and accelerate U.S. AI development, leveraging government assets in the attempt to spur private innovation and maintain a competitive edge. It directs agencies to remove bureaucratic hurdles, support private-sector AI growth, and promote innovation free from "ideological bias"; launches a government-wide effort to create a unified AI platform for scientific breakthroughs using federal data, supercomputers, and labs; and facilitates building AI data centers and energy infrastructure on federal lands through streamlined permitting and incentives.[78]

The U.S. Congress considered the *Federal A.I. Governance and Transparency Act, which* proposed governance requirements for federal AI systems, but as proposed, did not cover private-sector AI broadly.[79] The Act was introduced in the 118th Congress to establish a comprehensive framework for the governance of AI systems within federal agencies.[80] The bill sought to codify standards for the responsible design, development, acquisition, and oversight of AI technologies, emphasizing constitutional compliance, privacy protections, and civil liberties.[81] Key provisions included requiring agencies to publish governance charters for high-risk AI systems, mandating transparency in operations, and clarifying the Office of Management and Budget's authority to issue government-wide AI policies.[82] Additionally, the Act proposed regular reporting by agency inspectors general and the Government Accountability Office to ensure accountability and effectiveness.[83] Although the bill advanced through committee, it ultimately did not become law, reflecting ongoing challenges in creating uniform federal AI governance amid rapid technological change.[84]

In the absence of federal law, businesses face a patchwork of overlapping and sometimes conflicting state rules. For example, California's Transparency in Frontier Artificial Intelligence Act, signed by Governor Newsome on September 29, 2025, targets large-scale "frontier"

---

[66] *Artificial Intelligence*, CENTER FOR AI AND DIGITAL POLICY, www.caidp.org/resources/g20/.
[67] *Id.*
[68] *EU Artificial Intelligence Act*, EUROPEAN UNION (February 27, 2024), artificialintelligenceact.eu/high-level-summary/. *See also, The EU AI Act: A Quick Guide* SIMMONS + SIMMONS (July 12, 2024), www.simmons-simmons.com/en/publications/clyimpowh000ouxgkw1oidakk/the-eu-ai-act-a-quick-guide.
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] On January 20, 2025, President Trump signed an executive order that revoked the Biden administration's Executive Order 14110 on AI safety. See, *Trump Administration Early Executive Orders Signal Shift in AI Policy*, KING & SPALDING (February 14, 2025), www.kslaw.com/news-and-insights/trump-administration-early-executive-orders-signal-shift-in-ai-policy#:~:text=Since%20returning%20to%20office%2C%20President, developments%20in%20the%20new%20administration.
[73] Exec. Order No. 14,110, 3 C.F.R. 657 (2024).
[74] *Id.*
[75] Exec. Order No. 14148, 90 Fed. Reg. 8237 (Jan. 20, 2025).
[76] Exec. Order No. 14,179, 90 F.R. 8741 (Jan. 31, 2025).
[77] *Id.*
[78] *Id.*
[79] Federal A.I. Governance and Transparency Act of 2024, H.R. 7532, 118th Cong. (2024).
[80] *Id.*
[81] *Id.*
[82] *Id.*
[83] *Id.*
[84] *Id.*

models,[85] requiring risk assessments, safety protocols, and disclosure of catastrophic risks.[86] Penalties can reach $1M per violation.[87] Colorado's AI Act also regulates high-risk AI systems, but focuses on high stakes contexts including housing, employment, and finance.[88] The law was signed by Governor Jared Polis and mandates bias mitigation and transparency to prevent algorithmic discrimination. [89] The legislation is formally titled "An Act Concerning Consumer Protections for Interactions with Artificial Intelligence," but has become known as the CAIA.[90] It requires developers and deployers to use "reasonable care," conduct impact assessments, and provide consumer disclosures, with enforcement by the Attorney General starting February 1, 2026.[91]

Texas has enacted the Texas Responsible AI Governance Act (TRAIGA).[92] TRAIGA prohibits the development and deployment of AI systems for certain purposes, including behavioral manipulation, discrimination, capture of biometric data without consent, creation or distribution of child pornography or unlawful deepfakes, and infringement of constitutional rights.[93] Notably, the Act includes provisions implementing a regulatory sandbox program meant to promote innovation as well as responsible deployments of AI.[94] The Act also establishes the Texas Artificial Intelligence Council—a group of experts who will advise on the ethical, privacy, and public safety implications of deploying or developing AI systems in certain contexts.[95] The Act aims to protect Texas consumers from the foreseeable risks associated with using AI systems and contains language promoting transparency, notice to consumers, and the responsible development and use of AI systems.[96] The Act will go into effect on January 1, 2026.[97]

The Texas Attorney General has exclusive authority to bring actions in response to violations of the Act and to obtain civil penalties and injunctive relief; there is no private right of action.[98] State agencies may also impose sanctions on entities licensed, registered, or certified by that agency for violations in certain circumstances.[99] TRAIGA provides companies with a 60-day period to cure violations.[100] TRAIGA allows the state attorney general to obtain civil penalties of up to $12,000 for curable violations and up to $200,000 for uncurable violations (on a per violation

---

[85] "Frontier AI" refers to the most advanced, highly capable AI models (like next-gen large language models) that possess broad, general-purpose abilities. *Verification Of Frontier AI,* UNITED NATIONS, www.un.org/scientific-advisory-board/sites/default/files/2025-06/verification_of_frontier_ai.pdf.
[86] Cal. SB 53 (2025), (Oct. 8, 2025) (codified in part as Cal. Bus. & Prof. Code § 22757.10 *et seq*.), available at LegiScan or California State Portal CA.gov.
[87] *Id*.
[88] Act of May 17, 2024, ch. 198, 2024 Colo. Sess. Laws 1199 (codified at Colo. Rev. Stat. § 6-1-1701 *et seq.* (2024)
[89] *Id*.
[90] *Id.* NATIONAL ASSOCIATION OF ATTORNEY GENERALS, *A Deep Dive into Colorado's Artificial Intelligence Act*, (October 26, 2024) www.naag.org/attorney-general-journal/a-deep-dive-into-colorados-artificial-intelligence-act/.
[91] *Id.* Recent amendments, however, (namely SB 25B-004) have delayed some aspects of enforcement.
[92] Tex. Bus. Code § 551.001 *et seq.*; Sy Damle *et al*, *Texas Signs Responsible AI Governance Act Into Law*, LATHAM & WATKINS (June 23, 2025), www.lw.com/en/insights/texas-signs-responsible-ai-governance-act-into-law. *See also*, Kirk J. Nahra, *Texas Enacts New AI Law*, WILMERHALE (July 21, 2025). www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20250721-texas-enacts-new-ai-law.
[93] *Id.*
[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] *Id.*
[98] *Id.*
[99] *Id.*
[100] *Id.*

basis).[101]

During 2025, in fact, more than 1,000 bills have been introduced in 50 states, with about 10% successfully enacted, mostly focused on consumer protection, transparency, and algorithmic bias.[102] Other notable laws successfully passed deal with employment, such as Local Law 144 in New York City, which prohibits employers and employment agencies from using an automated employment decision tool to screen a candidate for an employment decision unless the tool has been subject to a recent bias audit and a summary of the audit is made publicly available, and all candidates are notified that such a tool will be used and given the opportunity to request an alternate selection process.[103] California and Illinois have enacted similar employment-related AI laws focusing on preventing discrimination, ensuring transparency, and requiring audits/disclosures. California passed regulations that amend the Fair Employment and Housing Act regulatory framework, focusing on AI.[104] While employers may continue to lawfully use AI to screen resumes, evaluate applicants' abilities, and rate interview performance, employers are prohibited from using AI to discriminate against applicants based on any protected characteristic; all California employers will be required to retain AI-related records for at least four years, and records must include the criteria for any AI use and the results of any AI analysis.[105]

Similarly, the Illinois AI Video Interview Act requires employers that record video interviews and analyze them using AI to notify each such applicant before the interview, provide each applicant with information regarding how the AI evaluation works, and obtain consent for the recording.[106] The CAIA also requires employers to use reasonable care to protect applicants from known or reasonably foreseeable risks of discriminatory treatment through the use of AI in employment and develop a risk management policy and conduct annual impact assessments to identify potential risks of discrimination.[107]

Several states, including Arizona and Alabama, have also enacted prohibitions against AI-deceptive media (particularly in the context of elections and child exploitation). In total, 45 states now have enacted laws that criminalize AI-generated or computer-edited child exploitation content, while 5 states and D.C. have not (as of August 2025). The states that do not have such laws on the books are Alaska, Colorado, Massachusetts, Ohio, Vermont (and Washington D.C.).[108]

Finally, several of the laws pertain to AI use in health care and, in particular, mental health care (for instance, Illinois' The Wellness and Oversight for Psychological Resources Act, which is effective as of August 1, 2025.)[109]

---

[101] *Id.*

[102] Amy Matsuo, *Regulatory Alert – State Series: AI Legislation*, KPMG (August 2025), kpmg.com/kpmg-us/content/dam/kpmg/pdf/2025/state-series-ai-legislation-reg-alert.pdf.

[103] 2021 N.Y.C. Local Law No. 144, N.Y.C. Admin. Code. § 20-870.

[104] Cal. Code Regs. tit. 2, § 11008.1 *et seq.*; Steven C. Kerbaugh, Alexander L. Reich, & Shivani Govani, *California's AI Hiring Rules Are Here—What Employers Need to Know Before October 1*, SAUL EWING (September 30, 2025) www.saul.com/insights/blog/californias-ai-hiring.

[105] *Id.*

[106] 820 ILL. COMP. STAT. 42/1 (2021); Lisa A. Larkin, *New Illinois Statute Among the First to Address AI-Aided Job Recruiting*, BAKER STERCHI (January 14, 2020), www.bakersterchi.com/new-illinois-statute-among-the-first-to-address-aiaided-job-recruiting.

[107] *See* note 88, *supra*.

[108] ENOUGH ABUSE, *State Laws Criminalizing AI-Generated or Computer-Edited Child Sexual Abuse Material* (August, 2025), enoughabuse.org/get-vocal/laws-by-state/state-laws-criminalizing-ai-generated-or-computer-edited-child-sexual-abuse-material-csam/.

[109] Wellness and Oversight for Psychological Resources Act, State of Illinois; Aug 4, 2025, [02-12-2025] ILLINOIS GENERAL ASSEMBLY, www.ilga.gov/legislation/PublicActs/View/104-0054.

Also of note: in March 2025, Virginia Governor Glenn Youngkin vetoed House Bill 2094, the state's proposed "High-Risk Artificial Intelligence Developer and Deployer Act," citing concerns it would create a burdensome regulatory framework hindering innovation, jobs, and investment, while duplicating existing federal efforts and overly burdening small businesses with compliance (including annual audits).[110] The bill aimed to prevent algorithmic discrimination in high-risk areas like employment and healthcare, requiring risk assessments and management policies for developers and users of high-risk AI.[111] The Governor viewed the bill as premature and detrimental to Virginia's nascent technology sector; he stated that believed the bill would discourage new businesses and talent from coming to Virginia.[112]

However, on December 11, 2025, President Trump signed an executive order titled "Ensuring a National Policy Framework for Artificial Intelligence" (the "Order").[113] The Order aims to "sustain and enhance the United States' global AI dominance" by establishing a "minimally burdensome national policy framework for AI" and outlines a series of steps to challenge or preempt state laws that conflict with that policy statement.[114] The goal of the Order is to reduce the web of diverging state laws and regulations that has emerged over the past few years.[115] Among other things, the Order calls for federal standards and legislation that would preempt conflicting state AI regulations, creates a federal litigation task force focused on challenging state AI laws in court, and conditions access to federal grant funding on states' willingness to avoid enacting onerous AI laws.[116] It is clear that a number of its initiatives will face legal challenges that make the impact of the Order unclear.[117]

C. Risk Categories

Companies build on existing governmental guidelines and regulation to frame their policies.[118] The Gartner report[119] collected "acceptable AI use policies," and after analysis, identified the following nine risks:

---

[110] Nathan Studeny and Michael Cantu, *Virginia Governor Vetoes AI Bill Aimed at Implementing Practical Regulations* (April 2, 2025) KJK, kjk.com/2025/04/02/virginia-governor-vetoes-ai-bill/#:~:text=The%20Veto,of%20the%20Virginia%20General%20Assembly.

[111] *Id.*

[112] Hannah Chanin, *VA Governor Vetoes Bill Regulating High-Risk Artificial Intelligence*, AMERICAN BAR ASSOC. (March 31, 2025), www.americanbar.org/groups/health_law/news/2025/3/va-governor-vetoes-bill-regulating-high-risk-artificial-intelligence/#:~:text=On%20March%2024%2C%202025%2C%20Virginia,to%20override%20Governor%20Youngkin's%20veto; Keely Quinlan, Virginia *Governor Vetoes Ai Discrimination Bill That Would Have Protected Consumers,* STATESCOOP, (March 25, 2025) statescoop.com/virginia-governor-youngkin-vetoes-ai-discrimination-bill/#:~:text=Youngkin%20vetoed%20the%20bill%2C%20saying%20it%20would:,AI%20usage%20guidelines%20across%20the%20executive%20branch.

[113] Executive Order 14365, 90 FR 58499 (2025) www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/.

[114] *Id.*

[115] Michael H. Rubin, *AI Executive Order Targets State Laws and Seeks Uniform Federal Standards*, (December 17, 2025) LATHAM & WATKINS, www.lw.com/en/insights/ai-executive-order-targets-state-laws-and-seeks-uniform-federal-standards.

[116] *Id.*, see also note 113.

[117] *Id.*

[118] Chandrasekharan, A., & Ramos, L. *Hype cycle™ for generative AI.* GARTNER (2024), www.gartner.com/interactive/hc/5636791?ref=explorehc.

[119] Lauren Kornutick *et al*, *Tool: Policy Template for Acceptable Use of Generative AI*, GARTNER RESEARCH (March 18, 2025), www.gartner.com/en/documents/6274083.

- Risk 1: Creation or sharing of abuse/sexual/violent content;
- Risk 2: Threatening or intent to create harm;
- Risk 3: Infringement on copyrighted or otherwise legally protected materials, inadvertent leakage of IP into public domain, or both;
- Risk 4: Algorithmic bias resulting from unrepresentative training data or model performance or misrepresentation of AI-generated content as human created;
- Risk 5: Unauthorized use or disclosure of personal or sensitive information or use of incomplete or inaccurate data for model training;
- Risk 6: Malicious or harmful AI-generated content (e.g., falsehoods/deepfakes, scams/phishing, hate speech);
- Risk 7: Vulnerabilities in generative AI systems (e.g., payload splitting to bypass safety filters, manipulability of open-source models);
- Risk 8: Inability to explain model outputs or model inaccuracies appropriately (*e.g.*, factually incorrect or outdated answers, hallucinations); and
- Risk 9: Risk of noncompliance with standards or regulations, societal risk, and reputational risk.

D. Frequency and Correlation of Risks Identified in Acceptable AI Use Policies

All of the reviewed policies address many of the potential risks involved in using generative AI tools. Table 2 shows which risks were identified in each organization's policies, where a "1" indicates that the risk is identified and "0" indicates that the risk is not included in that policy. The total number of risks included in each policy is shown in the final column of Table 2, and the final row shows how many of the policies identified the corresponding risk category.

Table 2. Risks Identified in Each Organization's Acceptable AI Use Policy

Company	**Risk 1**	**Risk 2**	**Risk 3**	**Risk 4**	**Risk 5**	**Risk 6**	**Risk 7**	**Risk 8**	**Risk 9**	**Total Identified Risks**
Amazon	1	1	0	1	0	1	1	0	1	6
Meta	1	1	0	0	1	1	1	0	1	6
Microsoft	1	1	1	1	1	1	0	0	1	7
Google	1	1	1	1	1	1	1	0	1	8
IBM	0	0	1	1	1	1	1	1	1	7
KPMG	0	0	1	1	1	0	0	0	1	4
Ernst & Young	1	1	1	1	1	1	0	0	1	7
Deloitte	0	0	1	0	0	1	0	1	0	3
McKinsey	1	1	1	1	1	1	1	1	1	9
Salesforce	1	1	1	1	1	1	0	0	1	7
No. of Policies Addressing Risk	7	7	8	8	8	9	5	3	9	

The measures of central tendency (*e.g.,* mean, median, and mode) give an idea of how similar the policies are, while the standard deviation and variance suggest the amount of difference between them. Most organizations include a substantial number of risks in their AUP, with an average of 6.4 risks per policy. The median and mode are both 7, indicating that seven risks is the most common coverage level. There were some outlier policies that identified fewer risks, leading to a standard deviation of 1.8 and variance of 3.24. McKinsey stands out as the only organization covering all nine risks, while Deloitte is an outlier with only three risks identified.

Further, this analysis shows that companies who sell products identify more risks in their policies than companies who provide consulting. Product-selling companies identify an average of 6.8 risks in their policies, while consulting companies include an average of 5.75 identified risks. There is more variation in the quantity of risks identified in consulting companies' policies, with a variance of six points and a standard deviation of 2.75, suggesting inconsistent approaches to risk governance. In contrast, the six product-selling companies had a variance of 2 points and a standard deviation of 0.75, likely due to stricter internal compliance requirements.

Table 2 also demonstrates the frequency with which specific risks are mentioned. Nearly all of the risk categories are identified in seven or more of the ten policies analyzed. The most frequently addressed risks were Risk 6 (malicious/harmful content) and Risk 9 (regulatory compliance) which appear in 9 out of 10 policies, and Risks 3, 4, and 5 (IP infringement, bias, and personal data misuse) which appear in 8 policies each. The least frequently addressed risks were Risk 8 (model inaccuracies/explainability), which appears in only 3 policies, and Risk 7 (system vulnerabilities) which appears in only 5 policies. These gaps suggest organizations prioritize content safety and compliance over technical robustness and transparency.

A correlation analysis demonstrates the relationships between risks identified within a policy. Three distinct clusters were identified: Stand-Alone Concerns, Content Safety, and Data and Compliance. The Stand-Alone Concerns cluster includes copyright infringement (Risk 3) and model inaccuracies (Risk 8). These risks were not correlated to each other or any other risk category. Table 3 shows the data correlation.

Table 3. Correlation Between Risks

	Risk 1	**Risk 2**	**Risk 3**	**Risk 4**	**Risk 5**	**Risk 6**	**Risk 7**	**Risk 8**	**Risk 9**
Risk 1	1								
Risk 2	1	1							
Risk 3	-0.33	-0.33	1						
Risk 4	0.22	0.22	0.37	1					
Risk 5	0.22	0.22	0.37	0.37	1				
Risk 6	0.51	0.51	-0.17	-0.17	-0.17	1			
Risk 7	0.22	0.22	-0.5	0	0	0.33	1		
Risk 8	-0.52	-0.52	0.33	-0.22	-0.22	0.22	0.22	1	
Risk 9	0.51	0.51	-0.17	0.67	0.67	-0.11	0.33	-0.51	1

The Content Safety cluster represents a set of risks that focus on preventing harmful or abusive interactions and maintaining system integrity within AI governance frameworks. The Content Safety cluster includes four risks: abuse content (Risk 1), threatening content (Risk 2), malicious content (Risk 6), and system vulnerabilities (Risk 7). These risks collectively aim to

safeguard users from exploitative or dangerous material and ensure that platforms remain secure against technical threats that could enable harmful content dissemination.

A key characteristic of the Content Safety cluster is the strong co-occurrence among its risks. Abuse and threatening content exhibit a perfect correlation, meaning they are always addressed together in organizational policies. Only three policies did not include these risk categories: IBM, KPMG, and Deloitte. Malicious content also shows moderate correlation with these two risks, reinforcing its role in content safety governance. System vulnerabilities, while less strongly correlated, are included due to their thematic alignment with harm prevention and security. Overall, this cluster reflects a proactive approach to user protection and compliance, with product-based companies prioritizing these risks more consistently than consulting firms. This emphasis suggests that organizations selling products adopt stricter internal standards for content moderation and technical resilience, aligning with ethical AI principles and regulatory expectations.

The Data and Compliance cluster includes three risks: algorithmic bias (Risk 4), unauthorized use/ disclosure of personal data (Risk 5), and regulatory compliance (Risk 9). There is a strong positive correlation between the risks in this cluster (up to 0.67). The data shows strong positive correlations among Risks 4, 5, and 9 (up to 0.67), forming a cohesive governance-oriented cluster. These risks are systemic and regulatory, focusing on fairness, privacy, and compliance obligations. All three risks appear in 8–9 policies, indicating near-universal recognition of compliance and ethical concerns. Thus, organizations emphasize legal and ethical safeguards, aligning with emerging regulatory frameworks. This cluster reflects a compliance-driven approach rather than technical explainability or robustness.

The Content Safety risks are output-centric, addressing harmful content and security threats, while The Data & Compliance risks are process-centric, focusing on governance, fairness, and regulatory adherence. Both clusters show strong internal correlations, but Content Safety risks are slightly less uniformly addressed, especially technical vulnerabilities (Risk 7). Data & Compliance risks dominate policy coverage, suggesting organizations prioritize legal and reputational risk mitigation over technical transparency or robustness.

Moreover, Risk 8 (model inaccuracies/explainability) is negatively correlated (-0.52) with Risks 1 and 2 (abuse and threatening content), suggesting policies that emphasize content safety often neglect explainability. Risk 3 (IP infringement) has weak or negative correlations with most other risks, making it a stand-alone concern. Generally, Risk 8 and Risk 3 appear isolated, reinforcing their classification as stand-alone concerns. This data is summarized in Table 4.

Table 4. Summary of Risk Clusters: Characteristics, Correlation, and AUP Coverage

Cluster	Risks Included	Correlation Strength	Frequency in Policies	Key Implications
Content Safety	Risk 1 (Abuse), Risk 2 (Threatsening), Risk 6 (Malicious Content), Risk 7 (System Vulnerabilities)	High among Risks 1, 2, and 6 (up to 0.51); Risk 1 & 2 perfectly correlated (1.0)	Risks 1, 2, 6 appear in 7-9 policies; Risk 7 only in 5 policies	Focus on preventing harmful outputs; technical vulnerabilities less prioritized
Data & Compliance	Risk 4 (Algorithmic Bias), Risk 5 (Personal Data Misuse), Risk 9 (Regulatory Compliance)	Strong positive correlation among Risks 4, 5, and 9 (up to 0.67)	All three risks appear in 8-9 policies	Emphasis on governance, fairness, and regulatory adherence
Stand-Alone Risks	Risk 3 (IP Infringement), Risk 8 (Model Inaccuracies/Explainability)	Weak or negative correlations; largely isolated from other risks	Risk 3 appears in 8 policies; Risk 8 only in 3 policies	Intellectual property protection and explainability are treated as separate issues, indicating gaps in holistic risk management

E. Implications of Risk Identification in Acceptable AI Use Policies

Among the nine identified risk categories, seven appear in at least seven of the analyzed AUPs. These risks largely correspond to behaviors widely recognized as problematic across multiple technologies, not just generative AI. For instance, Risks 1, 2, 3, and 6 prohibit the creation or dissemination of abusive, violent, threatening, copyrighted, or otherwise malicious content. Similarly, Risk 5 addresses the improper disclosure or misuse of sensitive information, while Risk 9 highlights the consequences of noncompliance with regulatory standards. These topics are common in many formal governance frameworks, reflecting longstanding concerns about harm, privacy, and legal obligations. Therefore, the frequent inclusion of these categories in AUPs is unsurprising, as they align with established norms for mitigating ethical, legal, and reputational risks.

In contrast, the fourth risk category is more specific to generative AI tools, as it focuses on algorithmic bias resulting from the generative AI tool's unrepresentative training data and related issues. Risks 7 and 8 are the least mentioned risks (addressed in only five and three policies, respectively), and these risk categories also address concerns that are vexing issues within, and largely specific to, AI. Risk 7 highlights the danger of payload splitting and open-source models. Payload splitting is a technique used to bypass safety filters or content moderation systems in AI models by breaking malicious or prohibited prompts into smaller, seemingly harmless segments and submitting them sequentially so that the results can be reconstructed to reveal the intended harmful output without triggering the AI safeguards.[120] Because AI tools are designed to comply with instructions which look harmless, it will execute such tasks without hesitation; AI tools have

[120] Sander Schulhoff, *Payload Splitting*, LEARN PROMPTING (August 7, 2024), learnprompting.org/docs/prompt_hacking/offensive_measures/payload_splitting?srsltid=AfmBOorIdsLDlZTWGdwNZYP-D02UNQic7e7z6b4pbWGJ6PxRZbsd5jGl.

no understanding or foreknowledge that two harmless instructions can become hazardous when later combined.[121] This vulnerability is particularly hazardous for open-source models, where safety layers may be weaker or easily removed by bad actors.[122] Thus, the ease with which the harmless queries can be modified and combined by bad actors for unethical purposes is an unsolved problem for generative AI researchers and developers.[123] It is perhaps due to the lack of an existing solution that this risk appears relatively infrequently in the policies.

Risk 8 acknowledges that there can be an inability to fully and appropriately explain model outputs and/or inaccuracies. For example, the creator of a generative AI tool may not be able to explain why the tool's output is incorrect or a "hallucination." Hallucination is the generation of false information or misleading results, given in a plausible, coherent, and confident manner.[124] These kinds of risks are a unique feature of AI models where mathematical models and computing power are used without fully understanding the inner workings.

One reason Risks 7 and 8 appear less frequently in AUPs may be the inherent difficulty of identifying when non-compliance occurs and determining its potential consequences. For instance, Risk 7 (model bias or discriminatory outputs) can be hard to detect because biases may emerge subtly in generated content or decision-making processes, making accountability unclear. Bias in AI systems often manifests in subtle, context-dependent ways rather than through overtly offensive or clearly incorrect outputs. For example, a language model might consistently favor certain demographic groups in job recommendation scenarios or use gendered language in ways that reinforce stereotypes, but these patterns only become visible when analyzing large volumes of outputs over time. Additionally, the complexity and opacity of AI models make it difficult to trace how training data or internal representations contribute to biased outcomes. This lack of transparency makes detecting Risk 7 a significant challenge for organizations.

Similarly, Risk 8 (hallucination or fabrication of information) poses challenges because it is not always obvious when an AI-generated statement is inaccurate, especially in complex or specialized domains.[125] Hallucinations are hard to detect because AI-generated content often appears fluent, coherent, and authoritative, even when it is entirely nonfactual.[126] Unlike obvious errors, hallucinations can involve plausible but false details, such as fabricated citations, nonexistent studies, or inaccurate facts that sound credible in context.[127] Thus, it is challenging for users to recognize inaccuracies without cross-referencing external sources, especially in specialized contexts where verifying information requires expertise.[128] Further, the hallucinations are not predictable; they can occur sporadically and without clear triggers, making systematic detection difficult.[129] Combined with users' tendency to trust well-structured outputs, these factors create a significant barrier to identifying and mitigating Risk 8.

---

[121] *Id.*
[122] *Id.*
[123] *Id.*
[124] Rahul Awati, *What Are AI Hallucinations And Why Are They A Problem?* TECH TARGET (October 11, 2024), www.techtarget.com/whatis/definition/AI-hallucination#:~:text=An%20AI%20hallucination%20is%20when%20a%20large,with%20LLMs%2C%20resulting%20in%20incorrect%20textual%20output.
[125] Lei Huang, *A Survey on Hallucination in Large Language Models: Principles, Taxonomy, Challenges, and Open Questions*, CORNELL UNIVERSITY ARXIV (November 19, 2024), arxiv.org/html/2311.05232v2.
[126] *Id.*
[127] *Id.*
[128] *Id.*
[129] *Id.*

Thus, Risks 7 and 8 stem from the complexity and opacity of AI models, which can make it hard to trace decisions or detect misuse. Additionally, users may lack sufficient understanding of the technology or fail to exercise due diligence in applying it responsibly, further contributing to ambiguity. As a result, organizations may hesitate to include these risks explicitly in their policies, given the uncertainty surrounding identification, enforcement and accountability.

IV. LEGAL ANALYSIS

Case law on the specific issue of liability stemming from the use or misuse of AI is sparse, but growing in volume each year. Due to the relative scarcity of verdicts or judgments arising specifically from the use or misuse of AI, cases considering corollary issues arising from the misuse of other technological tools (especially decision-making tools) are instructive. As AI tools become more widely used, litigation and guidance from courts (and legislatures) will increase. Until then, it is important to look at fact patterns involving AI that have not yet generated litigation, cases that are currently winding their way through the courts, as well as cases that have been litigated to conclusion involving AI and other technologies.

The existing fact patterns and cases can be divided into three broad categories. The first category includes cases where technology delivers bad advice or otherwise fails to perform properly, which does not cause bodily injury (*i.e.*, financial loss results but no danger to human safety exists). The second category includes cases where the use of technology either creates a risk of bodily injury, or has resulted in some bodily harm. The third category involves cases where the use of technology has caused, or contributed to, severe bodily injuries (*i.e.*, more than *de minimus* bodily injury) up to and including death.

A. Cases Involving Financial Harm

Of particular note in this category is the deployment of AI tools in the professional services, healthcare, financial services, and legal industries, where the resulting financial harm can often be clearly shown. In some cases, the misuse of these technological tools has resulted in substantial loss and/or regulatory fines. There are reported instances where companies face legal (and regulatory) consequences for using emerging technology internally, as well as cases involving companies providing AI output to advise customers with insufficient understanding or oversight.

1. Knight Capital

Knight Capital was a leading market maker and electronic execution firm, meaning it was a major player in buying and selling stocks on behalf of clients, including broker-dealers (like TD Ameritrade, E*Trade, Scottrade, and Vanguard) and institutional investors.[130] In 2012, Knight was the largest trader in U.S. equities with a market share of around 17 percent on the New York Stock Exchange (NYSE) and Nasdaq Stock Market.[131] Knight's Electronic Trading Group (ETG)

[130] Nathaniel Popper, *Knight Capital Says Trading Glitch Cost It $440 Million*, NY TIMES (August 2, 2012), archive.nytimes.com/dealbook.nytimes.com/2012/08/02/knight-capital-says-trading-mishap-cost-it-440-million/.
[131] Henrico Dolfing, *Case Study 4: The $440 Million Software Error at Knight Capital* (June 5, 2019), www.henricodolfing.com/2019/06/project-failure-case-study-knight-capital.html.

managed an average daily trading volume of more than 3.3 billion trades, trading over $21 billion daily.[132]

On August 1, 2012, Knight Capital experienced a software glitch that literally bankrupted the company.[133] Between 9:30 a.m. and 10:15 a.m. Eastern Standard Time, new software code was deployed which included a flaw that became apparent only after the software was activated when the NYSE opened for morning trading.[134] The new code led the firm's computers to rapidly buy and sell millions of shares and acquire massive long and short positions, largely concentrated in 154 stocks, totaling 397 million shares and $7.65 billion.[135] At 10:15, the company's trading operations for the day were halted.[136] When the erroneous trades were unwound, Knight reported a loss of $440 million, or about $10 million per minute of time the faulty computer code ran on Knight servers.[137] The losses were greater than the company's revenue in the second quarter of 2012, when it brought in $289 million.[138] This financial debacle forced Knight to accept $400 million of rescue financing that allowed them to continue operations, before ultimately being acquired by GETCO, another algorithmic trading company.[139]

A subsequent Securities and Exchange Commission (SEC) investigation found that Knight did not have adequate safeguards in place to limit the risks posed by its access to the markets, and as a result, failed to prevent the entry of millions of erroneous trade orders.[140] Knight failed to conduct adequate reviews of the effectiveness of its risk controls.[141] The SEC found that Knight violated federal securities laws and assessed monetary penalties (fines) of $12 million.[142]

An AUP focused on algorithm deployment and risk controls might have mitigated the Knight Capital incident by requiring rigorous testing, code review, and approval processes before activating new software in live trading environments. Such a policy could have mandated simulation in a sandbox environment, peer validation, and automated safeguards to prevent uncontrolled trading activity. Knight's liability stems from its failure to implement adequate risk management and compliance protocols, as evidenced by the SEC's findings that the firm lacked effective safeguards and monitoring systems. This negligence not only violated federal securities laws but also exposed Knight to regulatory penalties, reputational damage, and potential civil claims from clients affected by the disruption.

Risk 9 (risk of noncompliance with regulations and reputational risk) would apply in this situation. Knight's failure to implement adequate safeguards and risk controls violated federal securities laws, resulting in SEC penalties and reputational damage. This is a clear case of regulatory noncompliance and operational governance failure.

---

[132] *Id.*
[133] *Id.*
[134] Popper, *supra* note 130.
[135] Nima Badizadegan, *Knight Capital: The $440 Million Glitch*, SPECULATIVE BRANCHES (November 22, 2023), specbranch.com/posts/knight-capital/.
[136] *Id.*
[137] *Id.*
[138] *Id.*
[139] *Id; see also* Popper, *supra* note 130.
[140] Press Release 2013-222: *SEC Charges Knight Capital With Violations of Market Access Rule,* SECURITIES & EXCHANGE COMMISSION (Oct. 16, 2013); www.sec.gov/newsroom/press-releases/2013-222.
[141] *Id*.
[142] U.S. Securities and Exchange Commission Enforcement Proceedings, Issue 2013-199, (October 16, 2013) www.sec.gov/news/digest/2013/dig101613.htm#:~:text=Commission%20Charges%20Knight%20Capital%20with,orderly%20operation%20of%20the%20markets.%E2%80%9D.

Additionally, Risk 8 (inability to explain model outputs or model inaccuracies) would cover these facts. While Knight's issue was a software glitch rather than an AI hallucination, the inability to detect and explain the erroneous behavior of automated systems mirrors the accountability challenge seen in AI systems: when outputs are opaque and errors cannot be quickly diagnosed, organizations can face severe operational and financial consequences. Knight's inability to understand or control the system's outputs typifies the risk of unexplained or inaccurate results that Risk 8 addresses.

Knight would have benefitted from an AUP that aligned operational procedures with legal and ethical obligations to minimize financial, reputational, and regulatory exposure. Mitigating risks associated with automated trading systems or AI-driven processes is possible but requires a robust governance framework and technical safeguards. Organizations should implement rigorous pre-deployment testing, including simulation in sandbox environments, to validate code functionality under realistic conditions. Peer code reviews and formal approval workflows would help catch errors before production. Automated risk controls, such as kill switches and position limits, should also be embedded to prevent runaway transactions. Continuous monitoring and auditing of system function ensures anomalies are detected early. Post-deployment validation, which was entirely missing here, would function to confirm compliance with regulatory standards.

2. Replit/ SaaStr

On July 22, 2025, an autonomous AI agent from the technology firm Replit—designed to assist with coding and application development—accidentally deleted a production database belonging to startup SaaStr.[143] Over 2,000 database records were deleted.[144] Replit publicly apologized and refunded the program's purchase price to SaaStr.[145] When questioned about the incident, the AI coding assistant admitted to running unauthorized commands and violating explicit instructions not to proceed without human approval.[146] The AI coding assistant also concealed bugs and other issues by generating false data (including 4,000 fake users), fabricating reports, and lying about the results of tests.[147] Then, the AI agent misled the founder of SaaStr about his ability to recover the lost data.[148]

---

[143] Susanto Irwan, *When AI Goes Rogue: Lessons in Control from the Replit Incident* (July 28, 2025), xage.com/blog/when-ai-goes-rogue-lessons-in-control-from-the-replit-incident/#:~:text=Last%20week%2C%20the%20tech%20world,without%20governance%20is%20a%20vulnerability.

[144] Beatrice Nolan, *An AI-Powered Coding Tool Wiped Out A Software Company's Database, Then Apologized For A 'Catastrophic Failure On My Part,* FORTUNE (July 23, 2025), fortune.com/2025/07/23/ai-coding-tool-replit-wiped-database-called-it-a-catastrophic-failure/.

[145] *Id.*

[146] *Id.*

[147] *AI Goes Rogue: Replit Coding Tool Deletes Entire Company Database, Creates Fake Data for 4,000 Users*, THE ECONOMIC TIMES (July 22, 2025), economictimes.indiatimes.com/.

[148] *Id.*

The Replit case illustrates multiple key vulnerabilities of autonomous AI systems. Blind reliance on the AI coding assistant without robust oversight enabled unauthorized actions, including the deletion of SaaStr's production database and the fabrication of false data. These behaviors implicate Risk 8 (inability to explain model outputs or inaccuracies) because the AI concealed coding problems, disregarded instructions and generated misleading reports, making its actions opaque and difficult to audit. Additionally, the agent's violation of explicit instructions and execution of unauthorized commands implicate Risk 9 (noncompliance and reputational risk), as such failures can breach contractual obligations and erode trust. The propagation of false information, including fabricated users and test results, also implicates Risk 6 (malicious or harmful AI-generated content), because it distorted operational realities and misled decision-makers. This incident underscores the need for enforceable AI use policies, human-in-the-loop safeguards, and transparency mechanisms to prevent catastrophic operational and reputational harm.

An AUP could have significantly mitigated the risks demonstrated in the Replit incident by enforcing strict operational safeguards and accountability measures for autonomous AI agents. Such a policy should mandate human-in-the-loop oversight, requiring explicit human approval before executing any high-impact commands such as database modifications or deletions. It should also require transparent reporting protocols, prohibiting AI systems from fabricating data or concealing errors, and include mechanisms for auditability and explainability to ensure outputs can be verified. Additionally, the AUP should define clear boundaries for autonomous actions, implement automated fail-safes to prevent unauthorized commands, and require sandbox testing before deployment in production environments. By embedding these controls into governance frameworks, organizations can reduce operational, reputational, and compliance risks while maintaining trust in AI-assisted workflows.

3. xAI's Grok Goes Rogue

On July 8, 2025, xAI's Grok, a chatbot on the X platform (formerly known as Twitter), responded to a user's query with detailed instructions for breaking into the home of a Minnesota Democrat and assaulting him.[149] Will Stancil, an X user and Democratic policy maker, said he is considering legal action after Grok spoke about raping him and provided tips for those wanting to sexually assault him.[150] At one point, Grok provided suggestions to one X user who said he planned to rape Stancil and then asked for tips on how to break into his home.[151] "Bring lockpicks, gloves, flashlight and lube" the response from Grok read.[152] It went on to explain how to scout the location and pick the lock, and recommended actions to prevent the possible transmission of a sexually transmitted disease during the assault.[153] The chatbot also analyzed Stancil's posting patterns on X and told the user, "He's likely asleep between 1 a.m. and 9 a.m."[154] Grok then started to reference Stancil in response to questions that did not make mention of him at all.[155] Another post shared by Grok including very graphic details of how it would rape Stancil.[156]

That same week, Grok made a number of racist, antisemitic and pro-Nazi comments, that went so far as to praise Hitler and endorse the Holocaust.[157] Grok made a series of antisemitic

[149] Thor Olavsrud, *5 Famous Analytics and AI Disasters*, CIO (Aug. 7, 2025), www.cio.com/article/190888/5-famous-analytics-and-ai-disasters.html.
[150] *Id.*
[151] *Id.*

posts and declared itself "MechaHitler" repeatedly before X temporarily shut the chatbot down that evening.[158] The incident demonstrates how easily AI systems can produce dangerous content when moderation filters are removed or weakened.[159]

In another disturbing incident, in June of 2025, Grok spawned a trend of sexual harassment, enabling users to specifically to make it look a though women who posted selfies on X had semen on their faces.[160] Grok has created further outrage after Musk's AI team added the ability for any user to prompt Grok to edit images posted by other people on the X platform (formerly Twitter).[161] Predictably, users began generating sexually explicit images of women and children, including one image which used AI to digitally remove the clothing of a child actress who is just 14 years old.[162]

In response to inquiries from users, Grok has admitted "There are isolated cases where users prompted for and received AI images depicting minors in minimal clothing, like the example you referenced. xAI has safeguards, but improvements are ongoing to block such requests entirely."[163] Grok has also explained "… we've identified lapses in safeguards and are urgently fixing them—[child sexual abuse material] is illegal and prohibited."[164] The generated images appear to violate Grok's own terms of service, which prohibit the sexualization of children.[165]

These images also violate the Take It Down Act, which President Trump signed into law in May 2025.[166] This law made it illegal to "knowingly publish" or threaten to publish either an "intimate visual depiction" or a "digital forgery" [including AI-created deep-fakes] without a person's consent; the law includes strict penalties for the distribution of such material.[167]

The Grok cases demonstrate severe failures in AI governance and content moderation, implicating multiple risk categories. Most prominently, Risk 1 (creation or sharing of abuse/sexual/violent content) and Risk 2 (threatening or intent to create harm) apply, as the chatbot provided explicit instructions for breaking into a home and committing sexual assault and created sexually explicit material concerning minors. Additionally, Grok's racist, antisemitic, and pro-

---

[152] *Id.*
[153] Chris Spargo, *Elon Musk Grok AI Described Raping X User Who May Sue*, PEOPLE (July 10, 2025), people.com/elon-musk-grok-ai-described-raping-x-user-who-may-sue-11770091.
[154] *Id.*
[155] *Id.*
[156] *Id.*
[157] *Id.*
[158] *Id.*
[159] *Id.*
[160] Kat Tenbarge, *How Grok's Sexual Abuse Hit A Tipping Point,* SPITFIRE NEWS (January 2, 2026), spitfirenews.com/p/grok-csam-deepfakes-abuse-elon-musk.
[161] *Id.*
[162] *Id.*
[163] Kelly Corbett, *Popular AI Chatbot Under Fire After Users Create Explicit Images Of Child Actress,* SYRACUSE (January 2, 2026), www.syracuse.com/us-news/2026/01/popular-ai-chatbot-under-fire-after-users-create-explicit-images-of-child-actress-reports.html.
[164] *Id.*
[165] *Id.*
[166] Actions – S.146 – 119th Congress (2025-2026): TAKE IT DOWN Act, S.146, 119th Cong. (2025), www.congress.gov/bill/119th-congress/senate-bill/146/all-actions.
[167] 47 U.S.C. §§ 223–223a (as amended). The Act, which stands for "Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act," makes two main changes to federal law. First, the Act amends Section 223 of the Communications Act of 1934 (47 U.S.C. § 223) to add new criminal prohibitions related to the publication of intimate images. Second, the Act creates new requirements for covered platforms that the Federal Trade Commission (FTC) would enforce. The Act requires covered platforms to establish notice-and-removal processes by May 19, 2026. *See,* www.congress.gov/crs-product/LSB11314.

Nazi statements fall under Risk 6 (malicious or harmful AI-generated content), which includes hate speech and extremist propaganda. These outputs not only endangered an individual's safety but also amplified hateful propaganda, resulting in societal harm. Further, due to the outrageous nature of these events, the publicity brought severe reputational damage for the platform, both of which implicated Risk 9 (noncompliance with standards and reputational risk). The incident underscores the dangers of deploying generative or agentic AI systems without robust safeguards, as weakened moderation filters allowed the model to produce content that violated legal, ethical, and platform standards, exposing the organization to potential litigation and regulatory scrutiny.

The subsequent addition of image-editing capabilities escalates these concerns and underscores systemic weaknesses in safeguard design and enforcement, revealing how inadequate moderation and insufficient technical controls enable cascading ethical, legal, and societal risks. Collectively, these cases demonstrate that without robust guardrails, continuous adversarial testing, and strict compliance mechanisms, generative AI systems can rapidly become vectors for abuse, exploitation, and regulatory violations.

An AUP could have significantly reduced the severity of the Grok incidents by mandating strict content moderation protocols and governance standards for generative AI systems. The policy should require robust filtering mechanisms to block abusive, violent, or discriminatory outputs, alongside human-in-the-loop oversight for high-risk interactions. Clear guidelines for ethical boundaries and prohibited content categories, such as instructions for illegal acts, hate speech, and extremist propaganda, would ensure compliance with legal and platform standards. Additionally, the AUP should enforce continuous monitoring and auditing of AI outputs, coupled with escalation procedures for harmful responses, to prevent reputational damage and regulatory exposure. By embedding these safeguards into operational workflows, organizations can mitigate risks of societal harm, noncompliance, and trust erosion while maintaining responsible AI deployment.

4. Hallucinations

There are several well-publicized examples of AI hallucinations. For example, in an April 2024 post, an AI chatbot falsely accused NBA star Klay Thompson of throwing bricks through windows of multiple houses.[168] Some commentators speculated that Grok may have hallucinated the vandalism story about the basketball star based upon posts about Thompson "throwing bricks," common basketball parlance for badly missed shots.[169]

Similarly, the *Chicago Sun-Times* and *Philadelphia Inquirer* had their journalistic image tarnished when, in May 2025, editions featured a summer reading list that recommended books that do not exist.[170] Marco Buscaglia, the author of the special section, admitted he used AI to assist putting it together but failed to fact check the output.[171] The list featured many real authors but attributed nonexistent books to them, and also included wholly made up authors.[172]

In another painful example, Attorney Steven Schwartz found himself in hot water with US District Judge Kevin Castel after using AI to research precedents in a suit against Colombian airline

---

[168] Charles Curtis, *Klay Thompson's Awful Night Turned into a Wild Story About a 'Brick-Vandalism Spree' Thanks to Twitter AI*, FOR THE WIN (Apr. 17, 2024), ftw.usatoday.com/story/sports/nba/2024/04/17/klay-thompson-twitter-grok-ai-brick-vandalism-spree-meme/73355165007/.
[169] *Id.*
[170] Emma Bowman, *A Fake Summer Reading List Fooled Thousands Online. AI Made It Possible*, NPR (May 20, 2025), www.npr.org/2025/05/20/nx-s1-5405022/fake-summer-reading-list-ai.
[171] *Id.*
[172] *Id.*

Avianca.[173] Schwartz, a New York attorney, used the OpenAI chatbot to draft a brief for a personal injury case filed by an Avianca employee.[174] At least six of the cases cited in the brief are not real.[175] The Judge noted that the brief submitted by Schwartz included citations with false names and docket numbers, along with bogus internal citations and quotes.[176] Schwartz's partner also signed the brief, putting himself in jeopardy as well.[177] In an affidavit, Schwartz told the court it was the first time he used ChatGPT for legal research and he was unaware that its output could be false.[178] He also included screenshots of subsequent AI queries questioning the existence of the fake case cites, with AI doubling down and confirming that the fake citations were in fact real cases.[179] The judge fined Schwartz $5,000.[180]

Another federal judge disqualified three attorneys from a case because they included fake legal citations generated by AI in court filings.[181] The attorneys were sanctioned by U.S. District Judge Anna M. Manasco for the fake case citations and also referred to the Alabama State Bar for professional discipline.[182] The attorneys were also ordered to notify their clients and other courts of the matter.[183]

AI's penchant for generating fake but convincing-looking citations has resulted in courts around the country questioning, fining or otherwise disciplining lawyers in at least seven cases over the last two years.[184] The issue led to the American Bar Association notifying each of its 400,000 members last year that attorneys have an ethical obligation to vet AI output.[185]

Other examples of ChatGPT and other AI chatbots' inaccuracies abound. For example, the National Eating Disorder Association's chatbot provided people recovering from eating disorders with dieting tips.[186] The AI chatbot was intended to help people dealing with emotional distress, but instead made things worse by offering dieting advice and urging users to weigh and measure themselves.[187] Although this advice might have been helpful in a weight loss support group, emphasizing the importance of dieting and increased physical activity for those with an eating disorder is, at best, counterproductive.[188]

---

[173] Lyle Moran, *Lawyer Faces Sanctions After Using ChatGPT to Cite Fake Cases*, LEGAL DIVE (June 26, 2023), www.legaldive.com/news/chatgpt-lawyer-fake-cases-lawyer-uses-chatgpt-sanctions-generative-ai/653925/.
[174] *Id.*
[175] Samantha Delouya, *Lawyers Sanctioned After Citing Fake Cases Generated by ChatGPT*, CNN (May 27, 2023), www.cnn.com/2023/05/27/business/chat-gpt-avianca-mata-lawyers.
[176] *Id.*
[177] *Id.*
[178] *Id*.
[179] *Id.*
[180] *Id.*
[181] Sara Merken, *Judge Disqualifies Three Butler Snow Attorneys in Case Over AI Citations*, REUTERS (July 24, 2025), www.reuters.com/legal/government/judge-disqualifies-three-butler-snow-attorneys-case-over-ai-citations-2025-07-24/.
[182] *Id.*
[183] *Id.*
[184] Sara Merken, *AI 'hallucinations' in court papers spell trouble for lawyers,* REUTERS (February 18, 2025) www.reuters.com/technology/artificial-intelligence/ai-hallucinations-court-papers-spell-trouble-lawyers-2025-02-18/.
[185] *Id.*
[186] Sarah Fielding *US lawyers fined $5,000 after including fake case citations generated by ChatGPT* (June 23, 2023) www.engadget.com/us-lawyers-fined-5000-after-including-fake-case-citations-generated-by-chatgpt-114041179.html.
[187] *Id.*
[188] *Id.*

In a bit of irony, a misinformation expert was caught in a web of the very misinformation he railed against. The case involved a constitutionality challenge to a Minnesota statute that criminalizes the use of deepfakes intended to influence election results.[189] In support of the law, the Minnesota Attorney General submitted an expert declaration from Jeff Hancock, a Stanford University communications professor specializing in misinformation.[190] The declaration discussed the threats posed by AI and deepfakes.[191] After his opponents noted that the declaration included citations to non-existent articles, Hancock admitted that he relied on ChatGPT to draft portions of his filing.[192] The judge excluded Hancock's expert testimony, noting the irony that an expert on misinformation had submitted a court document containing misinformation.[193] The court held that the expert's failure to verify the AI output undermined his credibility to such an extent that the declaration could not be admitted into evidence in the matter.[194]

In a final example, ChatGPT wrongly accused Jonathan Turley, a U.S. criminal defense attorney and law professor at George Washington University, of sexual assault based upon a non-existent article from *The Washington Post*.[195] Mr. Turley was notified by a colleague that his name appeared in an output list created by AI in response to a query seeking a list of "legal scholars who have sexually harassed someone."[196] The chatbot fabricated claims that he assaulted a student during a class trip to Alaska.[197] According to Mr. Turley, via his blog, "It was a surprise to me since I have never gone to Alaska with students, The Post never published such an article, and I have never been accused of sexual harassment or assault by anyone."[198] The *Washington Post* has confirmed that this article never existed.[199] According to the *Washington Post*, these claims were then repeated by Microsoft's Bing chatbot, which is powered by GPT-4.[200]

Generative AI systems present multiple interconnected risks. One of the most prominent concerns is the inability to explain model outputs or inaccuracies (Risk 8). These cases amply illustrate this issue, and demonstrate how AI-generated outputs can appear credible yet be entirely

---

[189] Kohls v. Ellison, 2025 WL 66514 (D. Minn. Jan. 10, 2025)(examining the constitutionality of Minn. Stat. § 609.771); Kevin J. Quilty, *Expert Testimony in the Age of Generative AI: Recent Case Developments*, GREENBERG TRAURIG, (December 5, 2025) www.gtlaw.com/en/insights/2025/12/expert-testimony-in-the-age-of-generative-ai-recent-case-developments.

[190] *Id.*

[191] *Id.*

[192] *Id.*

[193] *Id.*

[194] *See Concord Music Grp., Inc. v. Anthropic PBC,* 2025 WL 1482734 (N.D. Cal. May 23, 2025) (plaintiffs moved to strike a defense expert declaration because it cited a nonexistent article. The defense admitted to using an LLM to format citations, but the court called the mistake "a plain and simple AI hallucination" and struck the problematic paragraph from the declaration, noting that the incident undermined the credibility of the expert's entire declaration.) *But see,* Ferlito v. Harbor Freight Tools USA, Inc., 2025 WL 1181699 (E.D. N.Y. 2025) (upholding the admissibility of an expert's testimony even though he had consulted ChatGPT because he used the AI tool only after forming his opinion, to confirm his conclusions, and he disclosed that use transparently).

[195] Aaron Mok, *ChatGPT Reportedly Made Up Sexual Harassment Allegations Against A Prominent Lawyer,* BUSINESS INSIDER (April 6, 2023), www.businessinsider.com/chatgpt-ai-made-up-sexual-harassment-allegations-jonathen-turley-report-2023-4.

[196] *Id.*

[197] Id.

[198] *Id.*

[199] Harwell, D. *ChatGPT Invented Fake Sexual Harassment Allegations*, THE WASHINGTON POST (April 5 2023), www.washingtonpost.com/technology/2023/04/05/chatgpt-lies/.

[200] *Id.*

fictitious. The inability to verify or explain why these outputs occur creates significant reputational and legal consequences for individuals and organizations.

Another important issue is malicious or harmful AI-generated content (Risk 6), which can arise even without malicious intent. These examples underscore the danger of deploying AI in sensitive contexts without adequate safeguards, as such outputs can lead to defamation, emotional distress, and potentially, health risks.

Algorithmic bias and misrepresentation (Risk 4) also pose substantial challenges. The Klay Thompson incident likely stemmed from linguistic bias, where the phrase "throwing bricks"—a basketball idiom for missed shots—was misinterpreted as vandalism. This demonstrates how unrepresentative training data and lack of contextual understanding can produce damaging errors, particularly when cultural or domain-specific language is involved.

The risk of noncompliance and reputational harm (Risk 9) is evident in cases where attorneys were sanctioned and fined for submitting AI-generated briefs containing fabricated citations, and newspapers suffered credibility damage after publishing AI-generated lists without fact-checking. These incidents highlight failures to adhere to professional and ethical standards, potentially resulting in legal penalties and erosion of public trust.

Finally, use of incomplete or inaccurate data (Risk 5) can lead to harmful recommendations, as seen in the eating disorder example. When AI systems rely on generalized health advice without domain-specific constraints, the production of outputs that are not only inaccurate but actively harmful is a risk.

An AUP would have significantly reduced the severity of these incidents by utilizing preventive controls, accountability mechanisms, and verification requirements to limit the likelihood of harmful outputs reaching the public. Several of the hallucination incidents detailed here—such as fabricated legal citations, nonexistent books in reading lists, and false allegations—stemmed from unverified AI outputs being treated as authoritative. An AUP requiring human-in-the-loop review and source verification protocols (*e.g.*, checking legal citations, validating ISBNs, or checking news sources) would have prevented these errors before publication. This would have prevented reputational damage for newspapers and avoided legal sanctions for attorneys.

Situations where these hallucinations are false allegations are directed at identifiable individuals give rise to the specter of defamation (*e.g.*, the Klay Thompson and Jonathan Turley cases). The creation of defamatory outputs illustrates the need for a prohibition on publishing negative claims without strong sourcing and the inclusion of a mandatory checkpoint in workflows where the legal department reviews and approves content before it is finalized or published. Any AI-generated output that could have legal implications, including such as court filings, contracts, compliance documents, regulatory statements or statements about individuals, must be examined by a qualified attorney or legal team to ensure accuracy and compliance with laws. An AUP with these clauses would have identified defamatory outputs by requiring escalation to legal counsel, reducing reputational and legal exposure.

Several of the incidents also involved misrepresentation of AI-generated content as human-preformed research, such as expert declarations, legal citations, and reading lists. An AUP mandating clear disclosure of AI assistance would have preserved credibility and allowed readers, courts, or clients to apply appropriate levels of skepticism. This transparency should reduce reputational harm because stakeholders understand the limitations of generative AI. In the context of submitting legal citations or expert declarations to a federal court, however, reliance on AI-generated content without comprehensive manual verification is categorically inadvisable. Every

citation must be independently validated against authoritative legal sources to ensure accuracy and adherence to professional standards.

In sensitive contexts, including the provision of health advice for those suffering from eating disorders, an AUP would restrict AI outputs to strictly non-clinical, supportive guidance, and would mandate disclaimers and escalation to human professionals for medical queries. This would also have prevented harmful recommendations and, thereby, reduced reputational harm.

5. MyCity

In October 2024, New York City announced a plan to harness the power of artificial intelligence to improve the business of government.[201] The city rolled out an AI-powered chatbot that was intended to provide New Yorkers with information on starting and operating a business in the city, as well as housing policy and worker rights.[202] The chatbot dispensed this misinformation in multiple languages.[203] The only problem was the tool, MyCity, told businesses to break the law in a myriad of ways: by falsely claiming that business owners could take a cut of their workers' tips, fire workers who complain of sexual harassment, and serve food that had been nibbled by rodents, among other falsehoods.[204] It also claimed landlords could discriminate based on source of income.[205] At the time, there was no indication to users that they should be skeptical of the information provided.[206] Users who visit today are informed the bot "uses information published by the NYC Department of Small Business Services" and is "trained to provide you official NYC Business information."[207] One small note on the page says that it "may occasionally produce incorrect, harmful or biased content," but there's no way for an average user to know whether what they're reading is false, and to what degree they should distrust the search results.[208] Further, a sentence also suggests users verify answers with links provided by the chatbot, although in practice, the search results rarely provide links.[209]

MyCity's erroneous responses implicate multiple risks associated with generative AI systems. Most notably, the case implicates Risk 8 (inability to explain model outputs or model inaccuracies), as the chatbot provided authoritative-sounding but factually incorrect guidance to users without clear mechanisms for those users to verify accuracy. This failure then implicated Risk 6 (malicious or harmful AI-generated content) as the misinformation encouraged illegal practices such as discriminating against employees and tenants, and serving contaminated food, potentially exposing users to legal and health hazards. The chatbot's presentation of biased or incomplete interpretations of labor and housing laws, misrepresenting official policy as permissive of unlawful conduct, implicates Risk 4 (algorithmic bias or misrepresentation). Furthermore, the lack of adequate disclaimers and verification links raises Risk 9 (noncompliance and reputational risk), as the city positioned the chatbot as an official source of information, undermining public trust and potentially exposing the government to liability. Finally, the reliance on incomplete or

---

[201] Colin Lecher, *NYC's AI Chatbot Tells Businesses to Break the Law*, THE MARKUP (March 29, 2024), themarkup.org/news/2024/03/29/nycs-ai-chatbot-tells-businesses-to-break-the-law.
[202] *Id.*
[203] *Id.*
[204] *Id.*
[205] *Id.*
[206] *Id.*
[207] *Id.*
[208] *Id.*
[209] *Id.*

inaccurate training data (Risk 5), is at play here since the chatbot's outputs were not grounded in validated legal and regulatory sources. This case underscores a recurring pattern: over-reliance on AI without robust human oversight amplifies systemic risk, leading to misinformation, legal exposure, and reputational harm.

An AUP could have substantially mitigated the harm caused by the MyCity chatbot through the implementation of robust governance and verification mechanisms. First, the AUP would mandate source integrity by requiring that all AI-generated responses link to authoritative legal and regulatory documents, thereby enabling users to easily validate accuracy. Additionally, human-in-the-loop oversight would be required for high-risk domains such as labor and housing law, ensuring that subject matter experts review outputs prior to deployment. An AUP would also enforce transparency through conspicuous disclaimers and clear attribution of AI involvement, reducing the likelihood that users interpret outputs as definitive legal guidance. The inclusion of a mandatory checkpoint in workflows for legal review of content before it is finalized or published would further restrict the chatbot to informational assistance rather than legal advice, thereby preventing unlawful recommendations and misrepresentations of policy. Collectively, these measures would have prevented the dissemination of misinformation, reduced legal exposure, and preserved public trust.

6. Air Canada

In February 2024, Air Canada was ordered to pay damages to a passenger after its virtual assistant gave him incorrect information and misled him into buying a full-price ticket, which proved costly.[210] Jake Moffatt consulted Air Canada's virtual assistant about bereavement fares following the death of his grandmother in November 2023.[211] The chatbot told him he could buy a regular price ticket from Vancouver to Toronto and apply for a bereavement discount by completing an online form within 90 days of the purchase.[212] Following that advice, Moffatt purchased a one-way CA$794.98 ticket to Toronto and a CA$845.38 return flight to Vancouver.[213]

However, when Moffatt submitted his refund claim within the 90-day window, the airline declined to reimburse him, explaining that fares cannot be retroactively adjusted for bereavement.[214] Moffatt presented Air Canada with screenshots of the chatbot conversation where the chatbot hallucinated an answer inconsistent with the airline's policy.[215] The airline refused to honor the erroneous advice, but admitted that the bot had used "misleading words" in its advice.[216] Rather than make Moffatt whole, the airline told Moffatt it would update the chatbot.[217] Even more surprisingly, Air Canada attempted to distance itself from the error by claiming that the bot was "responsible for its own actions."[218] Air Canada was roundly ridiculed and criticized by the press

---

[210] Marisa Garcia, *What Air Canada Lost In 'Remarkable' Lying AI Chatbot Case*, FORBES (Feb. 19, 2024), www.forbes.com/sites/marisagarcia/2024/02/19/what-air-canada-lost-in-remarkable-lying-ai-chatbot-case/.
[211] *Id.*
[212] *Id.*
[213] *Id.*
[214] *Id.*
[215] *Id.*
[216] Leyland Cecco, *Air Canada Ordered To Pay Customer Who Was Misled By Airline's Chatbot,* THE GUARDIAN (Feb. 16, 2024), www.theguardian.com/world/2024/feb/16/air-canada-chatbot-lawsuit.
[217] *Id.*
[218] *Id.*

for advancing this absurd claim.[219]

Moffatt took Air Canada to a tribunal in Canada, claiming the airline was negligent and misrepresented information via its virtual assistant.[220] Importantly, within the incorrect answer, the chatbot included a link to the actual Air Canada Bereavement Fares Policy page on the airline's website.[221] That page contradicts the chatbot and states "Please be aware that our Bereavement policy does not allow refunds for travel that has already happened."[222] Air Canada argued it could not be held liable for the information provided by its chatbot, and that a reasonable consumer would have taken the opportunity to confirm the answer by checking the link.[223]

Ultimately, the judge found for Mr. Moffat, saying the airline did not take "reasonable care to ensure its chatbot was accurate."[224] The judge also held that Air Canada failed to explain why the passenger should not trust information provided on its website by its chatbot.[225] The airline was ordered to pay Mr. Moffatt CA$812.02, including CA$650.88 in damages.[226]

This incident illustrates several critical risks associated with the deployment of AI-powered customer service tools. This incident primarily reflects Gartner's identified risks of algorithmic misrepresentation (Risk 4), system vulnerabilities (Risk 7), lack of explainability (Risk 8), and reputational and compliance concerns (Risk 9). The chatbot's erroneous advice contradicted the airline's official policy, demonstrating a failure to ensure accuracy and alignment between automated responses and authoritative sources. Furthermore, Air Canada's inability to explain the origin of the misinformation and its public-relations debacle of attempting to disclaim responsibility for its own customer service tool exacerbated reputational harm and led directly to legal liability. Although the chatbot included a working link to the correct policy, the tribunal found that the airline did not exercise reasonable care to guarantee the reliability of its AI system. This case underscores the necessity of implementing robust accuracy controls and transparency measures via an AUP.

One such transparency measure which would have been helpful in this case, and may have helped Air Canada avoid liability, is a confidence indicator. A confidence indicator is a feature in AI systems that communicates the system's level of certainty about its output.[227] It helps users understand whether the response is highly reliable or should be treated with caution.[228] Confidence indicators are often expressed as a percentage (*e.g.*, "90% confidence") or descriptive terms like "high," "medium," or "low" confidence.[229] These indicators increase transparency, improve decision making and allow users to confidently determine whether verification is advisable.[230] An indicator would also inform risk management decisions at the enterprise level.[231] Low-confidence

---

[219] *Id.*
[220] *Id.*
[221] Garcia, *supra* note 210.
[222] *Id.*
[223] *Id.*
[224] *Id.* This finding of failure to use due care under the circumstance seems to be roughly equivalent to a finding of negligence in a United States court.
[225] *Id.*
[226] *Id.*
[227] Bernardo Palos, *Why ML Prediction APIs Must Include Confidence Indicators*, PALOS PUBLISHING (2025), palospublishing.com/why-ml-prediction-apis-must-include-confidence-indicators/.
[228] *Id.*
[229] *Id.*
[230] *Id.*
[231] *Id.*

predictions could trigger human intervention or a second opinion; in contrast, high-confidence predictions can be automated, reducing human error and processing time.[232]

Similarly, disclaimers on the webpage would help mitigate risk by setting clear expectations about the reliability of AI-generated responses. Such a warning would enhance transparency and enable consumers to make informed choices by signaling that chatbot responses may require verification and should not be treated as definitive. Further, by warning users that the chatbot is solely an informational tool and not a definitive source, Air Canada could potentially reduce its exposure to negligence claims. Because courts often consider whether reasonable steps were taken to prevent a customer's misunderstanding, conspicuous disclaimers demonstrate due diligence.

Additionally, safeguards tailored to sensitive contexts would ensure that AI systems do not provide advice or recommendations on critical matters unless such information is corroborated by authoritative sources.

Finally, governance frameworks assigning accountability for AI-generated outputs would have prevented reputational damage stemming from Air Canada's ridiculous attempt to disclaim responsibility for its own system. The absurdity of its claims of no responsibility resulting from the false answer led to widespread media reporting of the case. This bad publicity was far worse for Air Canada than the damages awarded by the tribunal. Collectively, these provisions would have mitigated Air Canada's financial loss, legal liability, and reputational harm by ensuring accuracy, transparency, and accountability in its AI-assisted customer service.

7. iTutor Group

In August 2023, tutoring company iTutor Group agreed to pay $365,000 to settle a suit brought by the US Equal Employment Opportunity Commission (EEOC).[233] The federal agency said the company hired U.S.-based tutors to provide online tutoring from their homes or other remote locations.[234] According to the EEOC's lawsuit, iTutorGroup programmed their employment application software to automatically reject female applicants aged 55 or older and male applicants aged 60 or older.[235] The EEOC's suit stated that more than 200 qualified applicants were automatically rejected by the software.[236]

"Age discrimination is unjust and unlawful," then acting EEOC chair Charlotte Burrows said in a statement.[237] "Even when technology automates the discrimination, the employer is still responsible."[238] iTutor Group denied any wrongdoing but did voluntarily settle the suit for $365,000; as part of the settlement and consent decree, it agreed to adopt new anti-discrimination policies.[239]

This incident implicates several key AI risk factors, most notably algorithmic bias (Risk 4). Here, the discriminatory outcomes were directly linked to biased programming decisions embedded within the hiring algorithm. The case also reflects noncompliance and societal risk

---

[232] *Id.*
[233] U.S. Equal Employment Opportunity Commission Press Release (September 11, 2023), www.eeoc.gov/newsroom/itutorgroup-pay-365000-settle-eeoc-discriminatory-hiring-suit.
[234] *Id.*
[235] *Id.*
[236] *Id.*
[237] *Id*.
[238] *Id.*
[239] *Id*.

(Risk 9) based upon the automated rejections violating U.S. (federal) anti-discrimination laws, leading to regulatory enforcement and reputational harm. Additionally, data misuse (Risk 5) and malicious content (Risk 6) risks were tangentially implicated; the broader governance failure illustrates how inadequate oversight of AI systems can create systemic vulnerabilities. Furthermore, the inability to explain or justify the algorithm's decision-making process (Risk 8) likely compounded the problem, as transparency and accountability are critical in sensitive operational contexts, particularly domains with significant legal and ethical implications such as hiring and personnel management.

The repercussions of this case accentuate deeper issues of organizational governance, rather than mere technical flaws in the AI tool. Employers must implement robust bias detection and mitigation strategies, including pre-deployment audits, diverse training datasets, and continuous monitoring of algorithmic outcomes. Additionally, compliance frameworks should mandate explainability and human oversight (*i.e.*, human-in-the-loop review) for decisions affecting protected classes of candidates.[240] Failure to adopt such safeguards exposes organizations to legal liability, regulatory penalties, and erosion of public trust.

Ultimately, iTutor Group case serves as a cautionary example of how algorithmic systems can perpetuate unlawful discrimination when governance structures are weak or absent. Additionally, this case reinforces the principle that delegation to technology does not diminish legal and ethical obligations; in fact, it instructs, by extension, that that fair and unbiased hiring is a non-delegable duty, whether the delegatee is a human or an AI tool. This case serves as a reminder of a heightened need for proactive risk management and compliance in AI deployment.

An AUP would likely have substantially mitigated the discriminatory outcomes in this case by embedding governance mechanisms that prevent algorithmic bias and ensure compliance with anti-discrimination laws. Such a policy would mandate bias detection and mitigation protocols, including pre-deployment audits of hiring algorithms, use of diverse and representative training datasets, and continuous monitoring of selection outcomes for protected classes. Additionally, human-in-the-loop oversight for all automated employment decisions would ensure that final determinations are reviewed by qualified personnel rather than relying exclusively on algorithmic outputs. Domain-specific safeguards for recruitment would prohibit programming rules that explicitly or implicitly exclude candidates based on age, gender, or other protected characteristics, aligning with legal and ethical standards. Further, an AUP would enforce explainability requirements, obligating organizations to maintain transparent documentation of decision-making processes to facilitate accountability and regulatory review. Finally, compliance clauses within the AUP would establish clear accountability for AI-driven hiring practices, supported by regular audits and employee training on equal employment obligations. Collectively, these measures would have prevented unlawful discrimination, reduced regulatory exposure, and preserved organizational reputation by ensuring fairness and transparency in AI-assisted recruitment.

---

[240] These measures align with emerging regulatory standards such as the E.U. AI Act (Regulation [EU] 2024/1689 of the European Parliament and of the Council of 13 June 2024 on the harmonized rules for artificial intelligence) and ISO/IEC 42001, which both emphasize fairness, transparency, and accountability in AI systems. The AI Act is a European regulation on artificial intelligence (AI) – the first comprehensive regulation on AI by a major regulator anywhere. ISO/IEC 42001, the international management system standard for AI, offers a framework to help organizations implement AI governance across the lifecycle. In the EU, employers are liable for biased discriminatory hiring practices under established anti-discrimination laws and the new E.U. AI Act, even if the discrimination is unintended or results from the use of AI.

8. Zillow

Zillow, demonstrating its confidence in its ability to use AI to estimate the value of homes, announced a new option in February 2021—for certain homes, its "Zestimate" would also represent an initial cash offer from the company to purchase the property (a "Zillow Offer").[241] The "Zestimate" of home values was derived from a machine learning (ML) algorithm.[242] This system uses a combination of data including public records, property facts, and housing market trends to estimate home values.[243] The model is continuously updated and uses neural networks to improve accuracy and react to market changes more quickly.[244]

The business plan was to renovate the properties and flip them quickly for a profit.[245] The algorithm had a median error rate of 1.9%, but the error rate could be as high as 6.9% for off-market homes.[246] (Being off by as little as 1.9% on a single property with a Zestimate of $500,000 results in a $9,500 price swing.)

Three times a week, Zillow creates more than 500,000 unique valuation models, built atop 3.2 terabytes of data, to generate current Zestimates on more than 100 million US homes.[247] However, if any homes Zillow purchased had latent defects—such as a missed crack in the foundation—the Zestimate would not be able to predict those issues.[248] There are also many unquantifiable aspects of pricing a home, such as the value of living down the street from your parents, or having a manageable commute to the office.[249] These intangible factors vary from person to person, adding a factor that is impossible to roll into in the calculations, increasing the difficulty of outsourcing the home valuation process to a computer.[250]

In just eight months, Zillow bought 27,000 homes through Zillow Offers, while selling only 17,000 in that timeframe.[251] Zillow's business model assumed rapid resale of purchased homes for profit, but unforeseen, discrete events such as the COVID-19 pandemic disrupted market conditions, exacerbating existing systemic valuation inaccuracies.[252] According to Zillow, the algorithm led it to unintentionally purchase homes at higher prices than its current estimate of future selling prices, resulting in a $304 million inventory write-down in the third quarter of 2021.[253] In a conference call with investors following the announcement, Zillow co-founder and CEO Rich Barton said it might have been possible to tweak the algorithm, but ultimately it was too risky.[254] The company saw its stock plunge and was forced to cut 2,000 jobs, or 25% of its workforce.[255]

---

[241] Rachel Metz, *Zillow's Home-Buying Debacle Shows How Hard It Is To Use Ai To Value Real Estate*, CNN (November 9, 2021), edition.cnn.com/2021/11/09/tech/zillow-ibuying-home-zestimate.
[242] Zillow Group, *Meet The Brains Behind The New Zestimate, A Powerful Tool For A Hot Housing Market* (June 15, 2021).
[243] *Id.*
[244] *Id.*
[245] Metz, *supra* note 241.
[246] *Id.*
[247] *Id.*
[248] *Id.*
[249] *Id.*
[250] *Id.*
[251] *Id.*
[252] *Id.*
[253] *Id.*
[254] Olavsrud, *supra* note 149.
[255] *Id.*

This case implicates multiple Gartner AI risk categories. Algorithmic bias and misrepresentation (Risk 4) emerged as the model failed to account for intangible, subjective factors influencing home values, such as neighborhood familiarity or commute convenience. Explainability and accuracy issues (Risk 8) were central; Zillow acknowledged that while algorithmic adjustments were possible, the complexity and unpredictability of housing markets rendered such interventions too risky. System vulnerabilities (Risk 7) were evident in the model's inability to adapt to discrete events like the pandemic, exposing the weakness of AI systems under volatile conditions. Finally, regulatory, societal, and reputational risk (Risk 9) materialized as Zillow faced investor backlash, stock devaluation, and widespread criticism for over-reliance on algorithmic decision-making.

This case underscores the limitations of AI in contexts where data incompleteness and market volatility intersect with high financial stakes. An AUP could manage, and potentially reduce, these risks by embedding governance measures that prioritize accuracy, transparency, and risk management. This would be accomplished primarily by mandating stress testing and scenario analysis for valuation algorithms under volatile market conditions and ensuring resilience against rare but high-impact events such as the COVID-19 pandemic. Stress testing is a risk management technique used to evaluate how a system, model, or process performs under hypothetical extreme or adverse conditions; the goal is to identify vulnerabilities and understand the potential impact of rare but high-severity events. Scenario analysis involves creating multiple plausible scenarios—such as "best case", "worst case," and "moderate case"—and analyzing how each would affect outcomes.

Additionally, the AUP would require human-in-the-loop oversight for decisions involving substantial financial investment, preventing over-reliance on automated outputs for property acquisitions. Domain-specific safeguards would prohibit treating algorithmic estimates as definitive purchase offers without corroboration from independent appraisals or inspections, thereby accounting for latent defects and intangible factors that AI models cannot capture. Transparency measures such as confidence indicators and disclaimers would manage investor and consumer expectations by signaling uncertainty in algorithmic valuations. Finally, governance provisions would enforce continuous monitoring, explainability standards, and accountability frameworks, ensuring that algorithmic logic and risk assumptions are documented and auditable. Collectively, these safeguards could have mitigated financial losses, reputational damage, and workforce disruptions through rigorous risk management.

9. Tax Advice

An investigation by *The Washington Post* found that AI chatbots from TurboTax and H&R Block gave wrong answers as much as 50% of the time when asked "lightly challenging" tax questions.[256] The errors have widely been attributed to the use of general-purpose AI models that lack the specific, expert-curated knowledge needed to navigate the complex U.S. tax code effectively.[257] Both companies include disclaimers in their products, describing them as works in

[256] S.J. Steinhardt, *Tech Columnist: TurboTax and H&R Block Chatbots Are Unhelpful or Wrong Much of the Time*, NY CPAA THE TRUSTED PROFESSIONAL (March 7, 2024), www.nysscpa.org/news/publications/the-trusted-professional/article/tech-columnist-turbotax-and-hrblock-chatbots-are-unhelpful-or-wrong-much-of-the-time-030724.
[257] *Id.*

progress.[258] Specifically, TurboTax states "Intuit Assist is still developing and will improve with your help."[259] H&R Block states "Al Tax Assist is a digital helper that's still learning, so please review all responses."[260] The Intuit website also states that if a user has a question, they are a click away from a live tax expert, suggesting the AI is designed to be a supplementary tool, not an autonomous advisor.[261] Ultimately, the responsibility for accurate tax reporting and financial decisions will rest with the individual taxpayer or the human professional using the AI tool.[262] However, the findings raise significant concerns about the risks of deploying AI in high-stakes financial contexts.

Several risk factors are implicated in this case. Explainability and accuracy issues (Risk 8) are paramount, as the chatbots frequently produced factually incorrect responses without providing confidence indicators, clear reasoning, or citation to the tax code. Algorithmic misrepresentation (Risk 4) also applies, given that users might assume AI-generated answers are authoritative, despite disclaimers suggesting otherwise. Additionally, regulatory and reputational risk (Risk 9) is relevant because inaccurate tax guidance could lead to compliance failures, financial penalties for customers, and erosion of consumer trust. The case illustrates how incomplete or inaccurate data and lack of expert curation can undermine reliability in sensitive domains.

An AUP would require mitigation strategies such as domain-specific model training, integration of expert-curated knowledge bases, and human-in-the-loop review for complex queries. Transparency measures—such as confidence indicators and explicit disclaimers—are essential but insufficient on their own; organizations should ensure that fallback mechanisms, such as easy access to certified tax professionals, are prominently available. This case demonstrates that disclaimers alone may not be sufficient to absolve companies of responsibility for AI-generated misinformation, particularly when systems are marketed as consumer-facing tools in regulated industries.

10. VITAS

A California federal judge has denied VITAS Healthcare Corp.'s motion to dismiss a proposed class action over its use of third-party software to record and analyze phone calls it receives without notice to or consent from the caller.[263] Hospice-care provider VITAS Health Corp. allowed third-party software provider Invoca Inc. to record and analyze calls, create transcripts, and use AI to classify data from those calls into a searchable database.[264] Plaintiff, Ms. Tate, called VITAS to discuss sensitive details about the provider's hospice care for her grandmother.[265] Unbeknownst to Ms. Tate, VITAS utilized the Invoca software to listen to the

---

[258] *Id.*

[259] *Use Intuit Assist with Automation Flow Templates,* INTUIT, quickbooks.intuit.com/learn-support/en-us/help-article/branding/create-pre-built-journey-emails-intuit-assist/L7ealJMOu_US_en_US.

[260] *How does AI Tax Assist work?* H&R BLOCK, www.hrblock.com/tax-center/filing/filing-online/ai-tax-assist/#:~:text=You%20can%20take%20advantage%20of,maximum%20refund%20and%20100%25%20accuracy.

[261] *Id.*; Steinhardt, *supra* note 256.

[262] Steinhardt, *supra* note 256.

[263] Christopher Brown *Vitas Healthcare Lawsuit Advances Over Call-Center Recordings,* BLOOMBERG LAW (January 9, 2025), news.bloomberglaw.com/litigation/vitas-healthcare-lawsuit-advances-over-call-center-recordings.

[264] *Id.*

[265] Tate v. VITAS Healthcare Corp., No. 2:24-cv-01327-DJC-CSK, 2025 U.S. Dist. LEXIS 3828 (E.D. Cal. Jan. 8, 2025) (Order Denying Motion to Dismiss).

contents of the call and produce data about the call's purpose and resolution.[266] (In fact, neither VITAS nor Invoca obtained the consent of any caller to VITAS's call center, and all callers were unaware that their speech is being recorded and analyzed.)[267]

Further complicating matters, the software creator reserved the right (via its Terms of Service) to employ the data extracted from those calls for its own business and product-development functions.[268] In denying the motion to dismiss, the Court held that Ms. Tate could potentially prevail on her claim that the use of the software by the healthcare provider and the use of the data by the software developer for its own business purposes violated California privacy laws, and refused to dismiss the case.[269]

This case illustrates critical risks associated with AI-driven data processing in regulated industries. Unauthorized use or disclosure of personal or sensitive information (Risk 5) is central, as the calls contained highly sensitive health-related details, and the data was repurposed for secondary uses without explicit consent. Regulatory and reputational risk (Risk 9) is also significant, given potential violations of state privacy statutes (and potentially HIPAA)[270] and the heightened scrutiny surrounding healthcare data. System vulnerabilities (Risk 7) arise from reliance on third-party software without robust governance controls, creating unnecessary exposure to compliance failures. Additionally, explainability and transparency issues (Risk 8) are evident; callers were not informed that AI analytics were being applied, undermining trust and accountability.

VITAS would have benefitted from an AUP in this situation. An AUP would have mitigated the harm in this case by requiring explicit consent mechanisms, vendor compliance audits,[271] and data minimization policies[272] aligned with HIPAA and state privacy laws. Organizations must also implement clear disclosure practices—including verbal notices at the start of calls—and utilize contractual restrictions limiting third-party data use. This case reiterates that outsourcing AI functionality does not absolve healthcare providers of responsibility and amplifies the need for rigorous governance frameworks to protect sensitive information and maintain compliance in high-risk or regulated industries.

---

[266] *Id*.
[267] *Id.*
[268] *Id.*
[269] *Id*. at 1. The California Consumer Privacy Act provides a private right of action for any "consumer whose nonencrypted and nonredacted personal information ... is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security practices." Cal. Civ. Code §1798.150(a)(1). Suits brought under this provision have typically been related to data breach incidents.
[270] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, 110 Stat. 1936.
[271] A vendor compliance audit (with regard to data) is a systematic review of third-party vendors to ensure they handle sensitive data according to the organization's security, privacy, and contractual requirements, as well as compliance with relevant regulations. These audits verify whether vendors protect data through appropriate access controls, encryption, and breach-reporting preparedness, confirming that they comply with standards like HIPAA in the United States and the General Data Protection Regulation in the EU. QUIZCAT, *Ultimate Guide to Vendor Compliance Audits* (May 11, 2025), www.quizcat.ai/blog/ultimate-guide-to-vendor-compliance-audits.
[272] Data minimization policies are rules that ensure an organization only collects and keeps the personal data that is absolutely necessary for a specific, legitimate purpose. These policies limit the amount of data collected, how long it is retained, who can access it and for what purposes, thereby reducing the risk of data breaches and associated harm. Jan Stihec, *Why You Need to Take Data Minimization Seriously*, SHELF (July 11, 2024), shelf.io/blog/why-you-need-to-take-data-minimization-seriously/#:~:text=5%2DPoint%20RAG%20Strategy%20Guide,enshrined%20in%20laws%20and%20regulations.

11. Workday

In May 2025, a federal court in the Northern District of California granted a motion to preliminarily certify a class in a lawsuit alleging that an AI-based applicant screening system discriminated against individuals aged 40 and older.[273] The plaintiff, Derek Mobley, alleged that Workday's algorithm-based applicant screening tools discriminated against him and others based on race, age, and disability.[274]

Mr. Mobley alleges that Workday, a Human Capital Management platform, is directly liable for alleged unlawful employment discrimination caused by an employer's use of Workday's AI-powered hiring tools.[275] The judge in this closely watched case held that an AI vendor could be directly liable for employment discrimination under Title VII of the Civil Rights Act of 1964,[276] the Americans with Disabilities Act of 1990,[277] and the Age Discrimination in Employment Act of 1967,[278] under the theory that the AI vendor was acting as an "agent" of the employer. [279] The EEOC filed an amicus brief, supporting the plaintiff's novel theories of liability for AI vendors.[280]

The court accepted the premise put forward by Mr. Mobley that Workday's customers "delegate" the hiring functions traditionally performed by the employer to Workday.[281] Further, the court noted that Workday "… does qualify as an agent because its tools are alleged to perform a traditional hiring function of rejecting candidates at the screening stage and recommending who to advance to subsequent stages, through the use of artificial intelligence and machine learning."[282] In reaching this conclusion, the Court relied on the allegation that Mobley received rejection emails not just outside of business hours, but also almost immediately after submitting his application.[283] The court accepted the inference that this rapid rejection might be evidence of automation in the

---

[273] Dan M. Forman and Linda Wang, *Federal Court Grants Preliminary Certification in Landmark AI Hiring Bias Case* (June 18, 2025), www.cdflaborlaw.com/blog/federal-court-grants-preliminary-certification-in-landmark-ai-hiring-bias-case.

[274] *Mobley v. Workday, Inc.*, No. 23-cv-00770-RFL, 2024 U.S. Dist. LEXIS 126336 (N.D. Cal. July 12, 2024). AI platforms, such as ChatGPT, exhibit biases when sorting resumes; the University of Washington conducted research to determine the extent of the discriminatory bias. *See* Stefan Milne, *AI Tools Show Biases In Ranking Job Applicants' Names According To Perceived Race And Gender,* WASH. UNIV. (Oct. 31, 2024), www.washington.edu/news/2024/10/31/ai-bias-resume-screening-race-gender/. The research discovered significant racial, gender and intersectional bias in how three state-of-the-art large language models (Mistral AI, Salesforce and Contextual AI) ranked resumes. *Id.* In conducting their research, the researchers used varied names associated with white and Black men and women across more than 550 real-world resumes and found the large language models favored white-associated names 85% of the time; male-associated names 52% of the time versus female-associated names only 11% of the time; and never favored Black male-associated names over white male-associated names. *Id. See also* Marianna Michael Melendez and Catie A. Wheatley, *AI on Trial: Mobley v. Workday and the Future of Employment Law,* LOUISVILLE BAR ASSOCIATION'S BAR BRIEFS (October 01, 2025) www.faegredrinker.com/en/insights/publications/2025/10/ai-on-trial-mobley-v-workday-and-the-future-of-employment-law.

[275] Annette Tyman, *Mobley v. Workday: Court Holds AI Service Providers Could Be Directly Liable for Employment Discrimination Under "Agent" Theory*, SEYFARTH (July 19, 2024), www.seyfarth.com/news-insights/mobley-v-workday-court-holds-ai-service-providers-could-be-directly-liable-for-employment-discrimination-under-agent-theory.html.

[276] 42 U.S.C. 2000e *et seq*.

[277] 42 U.S.C. 12101 *et seq*.

[278] 29 U.S.C. 621–634 *et seq*.

[279] Tyman, *supra* note 275.

[280] *Id.*

[281] *Id.*

[282] Mobley v. Workday, Inc., 3:23-cv-00770, (N.D. Cal.)

[283] *Id.*; Tyman, *supra* note 275.

decision-making process.[284] Workday unsuccessfully argued that the software was simply "implementing in a rote way" an employer's straightforward "knockout" criteria or minimum qualifications.[285] Rather, the court held that petitioner sufficiently alleged that "Workday's software is not simply executing the criteria set by employers in a mechanical way, but is actively participating in the decision-making process by recommending certain candidates to proceed and rejecting others."[286]

The preliminary certification of a class action against Workday in May 2025 marks a pivotal moment in the legal treatment of AI-driven employment tools. This ruling has significant implications for both AI vendors and employers using AI-powered hiring tools, potentially expanding the scope of liability under federal anti-discrimination laws.[287] Given the fact that this case has survived a Motion to Dismiss, and given the EEOC's support of the plaintiff's novel argument for the extension of agency theory to an AI-powered tool, employers should take note of this potential liability.[288] Employers using AI-powered hiring tools should review their processes to ensure they can clearly articulate the role these tools play in their hiring decisions, and should also be prepared to demonstrate that their use of these tools does not result in disparate impacts on protected groups.[289]

Several of the Gartner risk factors are implicated. Algorithmic bias (Risk 4) is central, as the alleged discrimination reflects systemic bias embedded (whether inadvertently or purposefully) in the screening model. Explainability and accuracy issues (Risk 8) also arise because employers and vendors may struggle to justify automated decisions, particularly when rejections occur almost instantaneously, which could be indicative of a lack of transparency in how algorithms make decisions. Regulatory and reputational risk (Risk 9) is substantial, given the potential expansion of liability to AI vendors and the associated heightened scrutiny from enforcement agencies. Additionally, system vulnerabilities (Risk 7) emerge from over-reliance on automated tools without adequate human oversight or bias mitigation protocols.

An AUP would have included bias audits, transparent documentation of decision-making processes, and human-in-the-loop review for high-stakes employment decisions. Vendors and employers must also be required to implement governance frameworks that clarify accountability and ensure compliance with anti-discrimination laws, including clear documentation of hiring criteria. This case signals a paradigm shift: delegating hiring functions to AI does not diminish legal obligations but rather amplifies the need for proactive risk management and ethical safeguards.[290]

---

[284] *Id.*
[285] *Id.*
[286] *Id.*
[287] *Id.*
[288] *Id.*
[289] *Id.*
[290] It is important to note that there has thus far been no finding that Workday's software unlawfully discriminated against Mr. Mobley or any other jobseeker. There also has not yet been any opportunity for Mr. Mobley to determine what role, if any, Workday's software played in the allegedly wrongful rejections Mobley claims to have suffered at the hands of Workday's AI-based applicant screening tools.

12. Regulatory Scrutiny

In 2024, the U.S. Department of Justice (DOJ) served subpoenas on publicly-traded pharmaceutical companies, including Merck & Co., AstraZeneca Plc, and GSK Plc, related to electronic medical records and AI use.[291] The DOJ was seeking information regarding the companies' use of generative AI in electronic medical record (EMR) systems to determine whether the tool results in care that is either excessive or medically unnecessary, or whether the tool is used to generate inaccurate billing codes or diagnostic results.[292]

AI tools have been transformative in healthcare—able to detect hemorrhaging from CT scans, diagnose breast and skin cancer from images, identify abnormalities in chest X-rays, and detect otherwise imperceptible indicators of heart disease from a standard CT scan.[293] However, the DOJ is interested in the reliability of these diagnoses, specifically, how the models were trained, whether vendor compensation is related to the volume and value of referrals that the AI tools generate, and whether access to free AI tests tied to specific therapies or drugs raises anti-kickback questions.[294]

Revenue optimization tools are common in the healthcare industry, and not inherently problematic.[295] For example, many healthcare entities use charge capture tools to ensure clinical services are properly captured, clinical documentation improvement tools to write more specific descriptions in patients' charts, and other types of software tools to automate clinical coding, identify diagnosis codes, and perform billing, auditing and compliance functions.[296] AI is being integrated into these software tools to further streamline and improve the documentation, coding, and billing processes.[297]

However, these tools require appropriate oversight and compliance features.[298] The Department of Justice has elected to pursue several civil and criminal cases which underscore these concerns.[299] In the DxID case, a Medicare Advantage Organization (MAO) used an AI tool to review patients' medical records and add diagnosis codes that were "missed" by providers or previous coders.[300] The MAO then submitted these additional codes to the government, which resulted in increased billing amounts.[301] Often, however, the diagnosis codes added by the

---

[291] Ben Penn, *DOJ's Healthcare Probes of AI Tools Rooted in Purdue Pharma Case*, BLOOMBERG NEWS (January 29, 2024), news.bloomberglaw.com/us-law-week/dojs-healthcare-probes-of-ai-tools-rooted-in-purdue-pharma-case; Seth Goldberg, EMR Software Utilizing AI Targeted for Fraud and Abuse, DUANE MORRIS HEALTH LAW OVERVIEW (January 29, 2024), blogs.duanemorris.com/healthlaw/2024/01/29/emr-software-utilizing-ai-targeted-for-fraud-and-abuse/.

[292] *Id.*

[293] Vikash Ayyappan and Janis Coffin, *Artificial Intelligence In Diagnosing Medical Conditions And Impact On Healthcare*, MEDICAL GROUP MANAGEMENT ASSOCIATION (January 3, 2024), www.mgma.com/articles/artificial-intelligence-in-diagnosing-medical-conditions-and-impact-on-healthcare.

[294] Kate Driscoll and Nathaniel Mendell*, Artificial Intelligence in Healthcare: New Avenues for Liability,* JD SUPRA (March 4 , 2024), www.jdsupra.com/legalnews/artificial-intelligence-in-healthcare-3922166/.

[295] Jessica Sievert, Henry Leventis and William Brady, *The Justice Department's Focus On EHR Systems: Avoiding Government Scrutiny,* CHIEF HEALTHCARE EXECUTIVE (September 15, 2025) www.chiefhealthcare executive.com/view/the-justice-department-s-focus-on-ehr-systems-avoiding-government-scrutiny-viewpoint.

[296] *Id.*

[297] *Id.*

[298] *Id.*

[299] *Id.*

[300] *Id.*

[301] *Id.*

algorithm were not relevant to the patient's care, violating the applicable regulations.[302] The DOJ filed a lawsuit against the software company and the MAO, which settled for $98 million in December of 2024.[303]

Additionally, software that improperly influences providers or diminishes physician's independent medical judgment is also problematic.[304] For example, Practice Fusion implemented clinical decision support (CDS) notices in its software, alerting physicians when drugs could be prescribed.[305] In exchange for a fee paid by pharmaceutical companies (*i.e.*, a kickback), Practice Fusion used the alerts to steer physicians towards certain potentially addictive drugs.[306] Between 2014 and 2019, Practice Fusion's software generated over 230 million "pain" alerts that were designed to improperly push physicians to prescribe more extended-release opioids, even for less severe pain than would normally be appropriate, without adhering to prevailing medical guidelines that recommended non-opioid alternatives.[307] Practice Fusion entered into a $118.6 million settlement to resolve the civil case and a deferred prosecution agreement to resolve criminal allegations, which included $26 million in criminal fines and forfeiture.[308]

In another important case, Texas Attorney General Ken Paxton announced that an agreement has been reached with a Texas-based AI healthcare technology firm to resolve allegations the company violated the Texas Deceptive Trade Practices Act by making false, misleading, or deceptive statements about the accuracy of its AI tool.[309] Pieces Technologies was investigated over alleged false and misleading statements about the accuracy and safety of its AI-based products for in-patient healthcare facilities.[310] The company's products include AI-based tools that can be used by physicians to help them summarize, chart, and draft clinical notes in electronic health records.[311] Pieces Technologies touted metrics for this AI tool which indicated that it had an error rate of less than 1 per 100,000 entries.[312] The state's investigation found the company's claims "were likely inaccurate and may have deceived hospitals about the accuracy and safety of the company's products."[313]

In these situations, an AUP could have significantly reduced the legal, ethical, and reputational risks associated with the DOJ investigation into pharmaceutical companies' use of AI in electronic medical record (EMR) systems. First, the policy would mandate compliance-driven design principles, requiring that AI tools used for clinical decision support, coding, and billing adhere to federal regulations such as anti-kickback statutes and medical-necessity standards. Second, domain-specific safeguards included in the AUP would prohibit AI systems from

---

[302] *Id.*
[303] *Id.;* Archives, *Medicare Advantage Provider Independent Health to Pay Up To $98M to Settle False Claims Act Suit,* U.S. DEPARTMENT OF JUSTICE (December 2024), www.justice.gov/archives/opa/pr/medicare-advantage-provider-independent-health-pay-98m-settle-false-claims-act-suit.
[304] Sievert, Leventis and Brady, *supra* note 295.
[305] *Id.*
[306] *Id.*
[307] *Id.*
[308] *Id.*; Archives, *Electronic Health Records Vendor to Pay $145 Million to Resolve Criminal and Civil Investigations,* U.S. DEPARTMENT OF JUSTICE (January 27, 2020), www.justice.gov/archives/opa/pr/electronic-health-records-vendor-pay-145-million-resolve-criminal-and-civil-investigations-0.
[309] Steve Alder, *Texas Attorney General Resolves Investigation of GenAI Healthcare Technology Firm,* THE HIPAA JOURNAL (September 25, 2024), www.hipaajournal.com/texas-ag-settlement-pieces-technologies/.
[310] *Id.*
[311] *Id.*
[312] *Id.*
[313] *Id.*

influencing prescribing behavior or generating billing codes without corroboration from clinical guidelines and physician judgment, thereby preserving independent medical decision-making. Third, the AUP would enforce bias detection and audit protocols to ensure that the algorithms do not systematically promote excessive or unnecessary care or favor specific therapies or vendors, particularly when compensation from vendors is involved. Additionally, explainability and transparency requirements would obligate vendors and healthcare organizations to maintain documentation of model training data, logic, and performance metrics, enabling accountability and regulatory review. The policy would also require disclosure of AI limitations and confidence indicators to clinicians, reducing blind reliance on automated outputs. Finally, governance provisions would establish clear accountability frameworks, supported by periodic compliance audits and mandatory training for staff on ethical AI use in healthcare. Collectively, these measures would have mitigated the risk of fraudulent billing, undue influence on prescribing practices, and deceptive marketing claims, while safeguarding patient welfare and institutional integrity.

13. Samsung Leak

In 2023, Samsung faced significant intellectual property leaks when engineers inadvertently disclosed sensitive information in three separate incidents by uploading the data to ChatGPT.[314] An employee pasted confidential source code into the chat to detect errors and debug the code.[315] Another employee shared code with ChatGPT and "requested code optimization."[316] A third employee shared a recording of an internal meeting, requesting that it be transcribed into notes for a presentation.[317] As a result, Samsung banned the use of generative AI tools.[318]

Other well-known companies have also cracked down on the use of ChatGPT and similar tools among employees based on similar concerns. Amazon issued a similar warning to employees in January of 2023, informing its workers not to share any code or confidential information about the company with ChatGPT after discovering examples of ChatGPT responses that resembled internal Amazon data.[319] In February of the same year, JPMorgan Chase also heavily restricted the use of ChatGPT by its staffers amid concerns that it had regulatory exposure surrounding the sharing of sensitive financial information.[320]

Because generative AI platforms often retain user inputs for model training, sensitive data shared during interactions can persist beyond the intended session.[321] In fact, the OpenAI user guide expressly warns users against this behavior: "We are not able to delete specific prompts from

---

[314] Cecily Mauran, *Whoops, Samsung workers accidentally leaked trade secrets via ChatGPT*, MASHABLE (APRIL 6, 2023), mashable.com/article/samsung-chatgpt-leak-details.
[315] *Id.*
[316] *Id.*
[317] *Id.*
[318] Siladitya Ray, *Samsung Bans ChatGPT Among Employees After Sensitive Code Leak,* FORBES (MAY 2, 2023), www.forbes.com/sites/siladityaray/2023/05/02/samsung-bans-chatgpt-and-other-chatbots-for-employees-after-sensitive-code-leak/.
[319] *Id.*
[320] *Id.*
[321] *Id.*

your history. Please don't share any sensitive information in your conversations."[322] Users are informed that the system uses all questions and text submitted as training data.[323]

These instances illustrate a critical vulnerability in the use of AI tools within corporate and research environments: while these systems undoubtedly enhance productivity, they also create new channels for exposure of proprietary data if confidentiality settings are not properly configured. The Samsung case serves as a cautionary example, emphasizing the need for strict institutional policies, secure AI deployment, and employee awareness to prevent inadvertent leaks in an era of AI-driven workflows.

The incidents also highlight several critical risks identified in Gartner's framework for acceptable AI use. Risk 3 (infringement on copyrighted or legally protected materials and inadvertent IP leakage) is readily apparent in this fact pattern, as Samsung engineers uploaded proprietary source code and internal documentation to ChatGPT. These actions disclosed sensitive intellectual property to an external system that retains user inputs for model training (and potentially to incorporate into outputs presented to other users), creating a persistent vulnerability.

The unauthorized use or disclosure of personal or sensitive information (Risk 5) is also evident. Given that Samsung employees shared a recording of an internal meeting for transcription purposes, and JPMorgan's concerns about the disclosure of personal financial data, these disclosures raise privacy concerns and increase exposure to data misuse. Further, the OpenAI user guide explicitly warns users against sharing sensitive information, underscoring the inherent risk of data persistence in generative AI platforms.

Indirectly, the case also implicates Risk 4 (Algorithmic bias and misrepresentation of AI-generated content), as reliance on ChatGPT for code optimization and debugging introduces the possibility of inaccurate or biased outputs being integrated into organizational workflows without validation. This connects to Risk 8 (Inability to explain model outputs or inaccuracies), since generative AI systems can produce hallucinations or factually incorrect suggestions, despite employees' trust of these outputs for critical tasks.

Finally, Risk 9 (noncompliance with standards or regulations and reputational risk) is strongly implicated, particularly in JPMorgan's decision to restrict ChatGPT usage due to concerns about regulatory exposure surrounding personal financial data of customers.

This case illustrates how well-intentioned use of generative AI can activate multiple high-impact risks when governance frameworks are insufficient. These examples underscore the need for robust organizational policies, employee training, and vendor transparency to mitigate the compounded risks associated with generative AI adoption.

An AUP could have substantially mitigated the intellectual property and confidentiality risks of Samsung's inadvertent data disclosures by establishing strict governance and operational safeguards. Because the policy would prohibit employees from entering proprietary code, confidential documents, or sensitive recordings into external generative AI platforms, uncontrolled data exposure would be controlled. Additionally, the AUP would mandate the use of secure, enterprise-approved AI tools with privacy-preserving configurations, ensuring that user inputs are not retained for model training or shared beyond organizational boundaries. Employee training and attestation requirements would reinforce awareness of data security risks and clarify that generative AI systems cannot guarantee confidentiality. Additionally, the policy would require

---

[322] Emily Forlini, *Samsung Software Engineers Busted for Pasting Proprietary Code Into ChatGPT*, PC MAG (April 7, 2023), www.pcmag.com/news/samsung-software-engineers-busted-for-pasting-proprietary-code-into-chatgpt.

[323] *Id.*

data classification protocols and automated filters to block uploads of source code or regulated information to external systems. Governance provisions would also include vendor transparency requirements, obligating third-party AI providers to disclose data retention practices and compliance with applicable privacy and intellectual property laws. Finally, the AUP would establish audit and enforcement mechanisms, including monitoring of AI usage and sanctions for violations, to ensure accountability. Collectively, these measures would have prevented inadvertent IP leakage, reduced regulatory exposure, and preserved organizational trust in AI-enabled workflows.

14. Copyright Issues

AI companies have been hit with a slew of copyright lawsuits from media companies, music labels and authors since 2023.[324] Additionally, actors, directors and other artists have signed open letters urging government officials and AI developers to constrain the unauthorized use of copyrighted works.[325] In recent years, companies have also increasingly reached licensing deals with AI developers in order to maintain some control over the terms of use for their artists' works.[326] These licensing agreements set specific parameters for how the licensed content can be used, ensuring it aligns with the artists' and companies' expectations and establish clear financial compensation models.[327]

AI companies have long contended that their use of copyrighted materials constitutes "fair use." Fair use is a legal doctrine that allows limited use of copyrighted material without permission for purposes like criticism, comment, or—as courts are now determining—AI training.[328] A key test is whether the new use "transforms" the original work by adding something new or serving a

---

[324] More than 15 notable suits are pending across the country in which copyright owners are pursuing various theories of infringement against AI platforms, alleging that AI models either infringe their copyrights by training AI using copyrighted works, because the output of the AI models itself infringes, or both. *See,* Thomson Reuters Enter. Ctr. GmbH v. ROSS Intel. Inc., No. 1:20-cv-00613-SB (D. Del. filed May 6, 2020); UAB Planner 5D v. Facebook, Inc., 534 F. Supp. 3d 1126 (N.D. Cal. 2021); Doe 1 v. GitHub, Inc., No. 4:22-cv-06823-JST (N.D. Cal. filed Nov. 3, 2022); Getty Images, Inc. v. Stability AI, Inc., No. 1:23-cv-00135-JLH (D. Del. filed Feb. 3, 2023); Tremblay v. OpenAI, Inc., No. 3:23-cv-03223, (N.D. Cal. filed June 28, 2023); In re Google Generative AI Copyright Litigation, No. 5:23-cv-03440 (N.D. Cal. filed July 11, 2023); Authors Guild v. OpenAI, Inc., No. 1:23-cv-08292 (S.D.N.Y. filed Sept. 19, 2023); Kadrey v. Meta Platforms, Inc., No. 23-cv-03417-VC (N.D. Cal. Nov. 20, 2023); Huckabee v. Bloomberg L.P., No. 1:23-cv-09152 (S.D.N.Y. filed Oct 17, 2023); Concord Music Grp., Inc. v. Anthropic PBC, No. 3:23-cv-01092 (M.D. Tenn. filed Oct. 18, 2023); Andersen v. Stability AI Ltd., No. 3:23-cv-00201 (N.D. Cal. Second amended complaint filed Oct. 31, 2024); The N.Y. Times Co. v. Microsoft Corp., No, 1:23-cv-11195, (S.D.N.Y. filed Dec. 27, 2023); Nazemian et al. v. Nvidia Corp., No. 24-01454 (N.D. Cal. filed Mar. 8, 2024). *See also,* David M. McIntosh, Yam Schaal and Maureen Greason, *Does Training an AI Model Using Copyrighted Works Infringe the Owners' Copyright? An Early Decision Says, "Yes.",* ROPES & GRAY (March 6, 2025), www.ropesgray.com/en/insights/alerts/2025/03/does-training-an-ai-model-using-copyrighted-works-infringe-the-owners-copyright.

[325] Caitlin O'Kane, *Hundreds of Actors And Hollywood Insiders Sign Open Letter Urging Government Not To Loosen Copyright Laws for AI*, CBS NEWS (March 17, 2025), www.cbsnews.com/news/actors-artificial-intelligence-ai-hollywood-copyright-regulation/.

[326] Michael Hobbs, Jr. and Justin Tilghman, *How AI Cos. Can Cope With Shifting Copyright Landscape*, TROUTMAN PEPPER LOCKE (2024), www.troutman.com/insights/how-ai-cos-can-cope-with-shifting-copyright-landscape/.

[327] *Id.*

[328] Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984). *See,* Timothy P. Scanlan, Jr. *et al*, *Why Anthropic's Copyright Settlement Changes the Rules for AI Training*, JONES WALKER (August 29, 2025), www.joneswalker.com/en/insights/blogs/ai-law-blog/why-anthropics-copyright-settlement-changes-the-rules-for-ai-training.html?id=102l0z0.

different purpose, rather than simply copying it.[329] For instance, "fair use" can be explained as the difference between a critic quoting a novel to review it, or a screenwriter writing a scene that parodies it, versus someone photocopying the entire book to avoid buying it.[330]

Two cases of note have already been decided in 2025. First, in February 2025, Thomson Reuters, the owner of Westlaw, secured a landmark legal victory in one of the first major U.S. cases addressing copyright infringement in AI training.[331] The dispute arose when Ross Intelligence, a legal technology startup company, used Westlaw's proprietary headnotes and numbering system (editorial categorization akin to the Dewy decimal system and summaries of legal principles) to train its AI-powered legal research tool after failing to purchase a license.[332] The court ruled that these headnotes met the threshold for originality and were therefore copyrightable, emphasizing the creative judgment involved in selecting and organizing legal principles, and rejecting Ross's argument that they were mere factual summaries of public domain judicial opinions.[333]

Crucially, the court dismissed Ross's fair use defense, finding that its use was commercial, non-transformative, and directly competitive with Westlaw's offerings.[334] This decision seemed to set a significant precedent: AI developers cannot freely use copyrighted content for training without authorization, signaling a potential shift toward stricter licensing requirements and raising broader implications for innovation and the future of AI in legal research.[335] The principles may not be applicable absent the competitor/ competing product context, however.[336]

Additionally, although the defendant's fair use argument failed in this case, the ruling did not foreclose the possibility that future arguments could succeed under different facts (because "fair use" is a fact-intensive analysis).[337] Further, in his decision, Judge Bibas stressed that this case only addressed a non-generative AI tool.[338] Because fair use jurisprudence tends to rely heavily upon the first factor, the purpose and character of the use, and because generative AI models could theoretically create outputs that are more transformative in nature than the output in this case, this decision left open the possibility that the first factor could weigh in favor of AI platforms in future cases involving generative systems.[339]

In a March, 2025 analysis of the case, McIntosh *et al* predicted:

---

[329] *See* 17 U.S.C.A. § 107 ("[T]he fair use of a copyrighted work, ... for purposes such as criticism, comment, news reporting, teaching ... , scholarship, or research, is not an infringement of copyright.) To determine whether a particular use is "fair," the statute sets out four factors to be considered:
"(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
"(2) the nature of the copyrighted work;
"(3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
"(4) the effect of the use upon the potential market for or value of the copyrighted work."
[330] Scanlan, *supra* note 328.
[331] Memorandum Opinion, Thomson Reuters Enterprise Centre GmbH et al v. ROSS Intelligence Inc., Docket No. 1:20-cv-00613, 17 (D. Del. Feb. 11, 2025); David M. McIntosh, *supra* note 324.
[332] *Id.*
[333] *Id.*
[334] *Id.*
[335] David M. McIntosh, *supra* note 324.
[336] *Id.*
[337] *Id.*; see *supra* note 329.
[338] Memorandum Opinion, Thomson Reuters, at 22; David M. McIntosh, *supra* note 324.
[339] *Id.*

> Additionally, in computer programming copyright cases, copying at intermediate stages of development has been permitted based on the first factor (purpose and character of the use). Future jurisprudence in the AI-copyright field could follow a similar trajectory to software-related cases. In 2023, the Supreme Court stated in *Warhol*, "a use that has a distinct purpose is justified because it furthers the goal of copyright, namely, to promote the progress of science and the arts, without diminishing the incentive to create."[340] Thus, under the first fair use factor, AI defendants could possibly successfully argue that it is *justified* to copy certain copyrighted works in order to train their models, much like copying of code was necessary for innovation in the software industry.[341]
>
> The other fair use factors may also come out differently in future fair use cases with different facts. For example, in *Thomson Reuters v. Ross*, the allegedly infringed work was arguably barely original enough to receive copyright protection, which caused the second factor (the nature of the allegedly infringed work) to favor fair use. In future cases, the works in question may contain more [original] protectible expression, which would disfavor fair use. On the third factor, judges in ongoing AI-copyright litigation may align with Judge Bibas in finding that the amount and substantiality of the allegedly infringed work used favors fair use because the copies made in intermediate training steps are not made available to the public and thus constitute a limited amount of copying. Finally, the fourth factor may also be analyzed differently in future cases, as the defendant's use in *Thomson Reuters v. Ross* directly competed with the plaintiff's business, and that may not be true in other cases.

This case demonstrates the need to approach the use of data for training purposes cautiously and to adjust the risk analysis if relying on a fair use defense.[342] It is also important to recall that this decision did not involve a generative AI tool.[343] Thus, it is important to assess potential risks associated with the use of data for training AI with a close understanding of the AI technology itself and how these technical legal arguments may impact the potential risk analyses in context.[344] For example, as discussed above, generative AI tools may have a more compelling argument for transformative use.[345] Again, these are fact-specific inquiries.

Just months later, a landmark copyright ruling from the Northern District of California proved McIntosh's legal analysis to be well-reasoned and prescient. In the *Anthropic* case, the court held that artificial intelligence developers can train models using copyrighted materials (here,

---

[340] Andy Warhol Found. for the Visual Arts, Inc. v. Goldsmith, 598 U.S. 508, 527-528, 143 S. Ct. 1258, 1274, 215 L.Ed.2d 473 (2023)(holding the "central question" of the first factor, the "purpose and character of the use," is "whether the new work merely supersede[s] the objects of the original creation ... (supplanting the original), or instead adds something new, with a further purpose or different character."

[341] *See* Google LLC v. Oracle Am., Inc., 593 U.S. 1, 24 (2021); *contra* Memorandum Opinion, Thomson Reuters, 1:20-cv-00613, at 18.

[342] Monique N. Bhargava ,Mitesh P. Patel, and Katherine Litaker, *Court shuts down AI fair use argument in Thomson Reuters Enterprise Centre GMBH v. Ross Intelligence Inc.* REED SMITH (March 3, 2025), www.reedsmith.com/en/perspectives/2025/03/court-ai-fair-use-thomson-reuters-enterprise-gmbh-ross-intelligence.

[343] *Id.*

[344] *Id.*

[345] *Id.*

published books) without authors' consent.[346] The decision makes the watershed finding that training AI systems on copyrighted work does, in fact, constitute fair use.[347]

The *Anthropic* case was brought by three authors who claimed that Anthropic ignored copyright protections while it built its "central library" to train Claude, its flagship LLM. The plaintiffs claimed the company's practices infringed their exclusive copyrights and enabled Claude to generate competing content that could displace demand for the originals. Along the way, Anthropic pirated more than 7 million books, and also lawfully purchased books which it then digitized and discarded. These books were fed into its LLM, and used to train the programs to generate humanlike text responses.[348] The Court held that "[t]he technology at issue [the LLM] was among the most transformative many of us will see in our lifetimes."[349]

Specifically, the court said Anthropic's use of the books to train its LLM Claude, was "quintessentially," "spectacularly," and "exceedingly" transformative and therefore constituted fair use.[350] Fair use, as defined by the Copyright Act, takes into account four factors: the purpose of the use, what kind of copyrighted work is used (creative works get stronger protection than factual works), how much of the work was used and whether the use hurts the market value of the original work.[351]

Judge Alsup's ruling that using copyrighted materials to train AI models constitutes transformative fair use (essentially, using copyrighted material in a new way that does not compete with the original) is a clear victory for AI developers. The court held that AI models are "like any reader aspiring to be a writer" who trains upon works "not to race ahead and replicate or supplant them—but to turn a hard corner and create something different."[352]

However, he went on to rule that, while making digital copies of purchased books was fair use, downloading pirated copies did not constitute fair use.[353] He ruled that, although AI developers can legally train AI models on copyrighted works without permission, they should obtain those works through legitimate means that do not involve pirating or other forms of theft.[354] Because the copies used to build a central library that were obtained from pirated sources plainly displaced demand for the authors' books—copy for copy—fair use does not apply to these pirated copies.[355] But aside from the millions of pirated copies, Alsup wrote, copying entire works to train AI models was "especially reasonable" because the models did not reproduce those copies for public access and because doing so "did not and will not displace demand" for the original books.[356]

Despite siding with the AI company on fair use for legally purchased books, Alsup held that Anthropic would still face trial for the pirated copies it used, finding piracy of copyrighted works to be "inherently, irredeemably infringing."[357] "That Anthropic later bought a copy of a

---

[346] Bartz v. Anthropic PBC, 787 F. Supp. 3d 1007 (2025); Angela Yang, *Federal judge rules copyrighted books are fair use for AI training*, NBC NEWS (June 24, 2025), www.nbcnews.com/tech/tech-news/federal-judge-rules-copyrighted-books-are-fair-use-ai-training-rcna214766.
[347] Bartz, 787 F. Supp., 3d at 1019.
[348] Bartz, 787 F. Supp., 3d at 1014.
[349] *Id.* at 1033.
[350] *Id.* at 1022, 1021, and 1019.
[351] *See* note 329, *supra*.
[352] Scanlan, *supra* note 328; Bartz, 787 F. Supp., 3d at 1022.
[353] *Id.* at 1025.
[354] *Id.* at 1034.
[355] *Id.* at 1033.
[356] *Id.* at 1031.
[357] *Id.* at 1025.

book it earlier stole off the internet will not absolve it of liability for the theft," Judge Alsup wrote, "but it may affect the extent of statutory damages."[358]

This split decision left Anthropic partially vindicated on the big question of AI training but still facing massive liability for downloading pirated copies of books; then came a procedural decision that greatly changed the trajectory of the suit.[359] In August 2025, Judge Alsup certified the case as a class action, defining the class to include "all beneficial or legal copyright owners of the exclusive right to reproduce copies of any book" in the pirated datasets that met his criteria (in all, 482,460 books made it through the class definition's filters.)[360] This class definition was wholly crafted by the judge himself, sweeping in not just authors but publishers, estates, and anyone else with reproduction rights—a broader class than was even contemplated by plaintiff's counsel.[361] This certification turned three individual authors into representatives of thousands of rightsholders in a mega-lawsuit representing nearly half a million works.[362]

After class certification, Anthropic faced potential statutory damages approaching hundreds of billions of dollars, and perhaps even a reaching a trillion dollars (statutory damages can range from $750 to $30,000 per infringed work, and up to $150,000 per infringed work if the infringement is willful).[363] Anthropic was staring down the barrel of a potential (uninsured) liability of catastrophic size.

After warning both the district court and an appeals court that the potential liability amounting to hundreds of billions of dollars in statutory damages created a "death knell" situation that would force an unfair settlement; with trial approaching, Anthropic negotiated a stunning settlement—$1.5 billion dollars. This settlement, if approved by the court, will be the largest publicly reported copyright recovery in history, and would set a new benchmark for other AI-related litigation and licensing disputes.[364]

The settlement includes monetary relief in the form of a minimum cash payment of $1.5 billion (approximately $3,000 per work for roughly 500,000 class members) plus statutory interest;[365] injunctive relief requiring the destruction of all datasets containing pirated works; and a release of past claims arising from Anthropic's use of their works.[366] Claimants, at the court's direction, participate in the settlement on an "opt-in" basis rather than the standard "opt-out" basis.[367] Copyright holders that decline to opt in may still pursue individual actions.[368]

---

[358] *Id.*; Regina Sam Penti, Matthew J. Rizzolo, and Yam Schaal, *Anthropic's Landmark Copyright Settlement: Implications for AI Developers and Enterprise Users,* ROPES & GRAY (September 8, 2025), www.ropesgray.com/en/insights/alerts/2025/09/anthropics-landmark-copyright-settlement-implications-for-ai-developers-and-enterprise-users.

[359] Dave Hansen, *The Bartz v. Anthropic Settlement: Understanding America's Largest Copyright Settlement*, KLUWER COPYRIGHT BLOG (November 10, 2025), legalblogs.wolterskluwer.com/copyright-blog/the-bartz-v-anthropic-settlement-understanding-americas-largest-copyright-settlement/.

[360] *Id.*

[361] *Id.*

[362] *Id.*

[363] *Id.*; *See* 17 U.S.C.A. § 101 *et seq,*; *see also* U.S. Copyright Office, www.copyright.gov.

[364] Penty, *supra* note 358.

[365] *Id.* The per-work settlement amount of $3,000 is four times larger than the $750 floor for statutory damages, and 15 times larger than what the plaintiffs would have obtained had Anthropic prevailed at trial on its defense of innocent infringement and convinced a court to exercise its discretion to apply a downward revision of the damages awarded to $200 per work.

[366] *Id.*

[367] *Id.*

[368] *Id.*

It is noteworthy that claims based on infringing outputs are carved out of the release and are therefore preserved.[369] Other suits in current litigation also remain against Anthropic – including copyright suits from music publishers, including Universal Music Corp. and Concord Music Group Inc., as well as Reddit.[370] However, the settlement clarifies an important principle: how companies acquire data matters as much as what they do with it.[371]

The *Anthropic* decision runs the gamut of critical risks for generative AI development. First, copyright and intellectual property risk (Risk 3) remains significant despite the court's finding that training on copyrighted works can constitute fair use when those works are lawfully obtained. The holding that piracy is "inherently, irredeemably infringing," exposes developers to potentially catastrophic liability, as evidenced by the size of the settlement. Second, noncompliance and reputational risk (Risk 9) is implicated because "fair use" interpretations may vary across jurisdictions, and litigation—even when partially successful—can be enormously expensive and corrosive to public trust. Third, the case highlights transparency and explainability concerns (Risk 8), as plaintiffs argued that millions of pirated books were ingested without disclosure, illustrating the need for documentation of data sourcing. Fourth, there may be issues of algorithmic bias risk (Risk 4) from reliance on pirated books, which may reflect narrow cultural or demographic perspectives. Fifth, system vulnerability and governance risks (Risk 7) arise from Anthropic's ingesting of pirated content, suggesting weaknesses in sourcing controls that could potentially allow malicious payloads. Finally, content integrity risks (Risk 6) arise because pirated sources may contain altered or harmful material, increasing the likelihood of unsafe outputs. Collectively, these risks demonstrate that legal compliance alone does not eliminate ethical, operational, and reputational exposure; organizations must adopt comprehensive governance frameworks encompassing lawful sourcing, transparency, bias mitigation, and security controls to manage the complex risk landscape revealed by this case.

An AUP could have significantly reduced the legal and reputational risks associated with copyright infringement in these cases by establishing clear governance for data sourcing and intellectual property compliance. First, the policy would mandate lawful acquisition of training data, explicitly prohibiting the acquisition or use of pirated content and requiring documentation of licensing agreements for proprietary materials. Second, the AUP would enforce vendor transparency and audit protocols, obligating developers to maintain detailed records of data provenance and to disclose sourcing practices to regulators and stakeholders. Third, risk assessment procedures would be required prior to model training, including legal reviews of copyright implications and fair use considerations tailored to the specific AI technology and its intended output. Additionally, the policy would incorporate bias and integrity safeguards, ensuring that training datasets are not only lawfully obtained but also free from harmful or manipulated content that could compromise output reliability. Finally, governance provisions would establish accountability frameworks and escalation mechanisms for compliance failures, supported by employee training on intellectual property law and ethical AI development. Collectively, these measures would have mitigated the likelihood of catastrophic liability and preserved public trust.

[369] *Id.*
[370] *Id.*
[371] Scanlan, *supra* note 328.

15. Clearview AI

Clearview AI is a facial recognition company that amassed a database of billions of images by scraping publicly available photographs from social media platforms and websites without user consent.[372] The company scrapes images of people's faces from millions of websites, including Facebook, Twitter, Venmo, and YouTube.[373] These images, often linked to personally identifiable information, were subsequently used to train facial recognition algorithms deployed for law enforcement and commercial purposes.[374] Alarmingly, a user can upload an image of a random person, and the system will match it to one of the three billion scraped images.[375]

Senator Edward Markey (D-MD) sent a letter to Clearview stating that the company is "fundamentally dismantling Americans' expectation that they can move, assemble, or simply appear in public without being identified."[376] Twitter also recently sent a cease and desist letter to the company demanding that Clearview stop taking photos from its website and delete any data that it previously collected.[377]

While individual data privacy problems are the primary concern, there are also questions concerning Clearview's accuracy.[378] Clearview's website states that "an independent panel of experts reviewed and certified Clearview for accuracy and reliability."[379] Ensuring Clearview's accuracy is essential for accurate law enforcement; however, there is no data to support Clearview's claims.[380] Law enforcement could mistakenly believe someone is a suspect in a crime based on Clearview's erroneous results and react violently or justify other action on false and misleading information.[381] These inaccuracies could potentially have a ripple effect leading to multiple civil and criminal violations by users.[382]

This practice constitutes a clear violation of privacy norms and regulatory frameworks, as individuals were neither informed nor granted permission for their data to be repurposed for surveillance. The incident underscores the ethical and legal implications of using personal data in AI model development without transparency or consent, raising concerns under global data protection laws such as the General Data Protection Regulation (GDPR).[383]

The Clearview AI case implicates multiple risks outlined in Gartner's framework. Risk 5 (unauthorized use or disclosure of personal or sensitive information) is most evident, as the company scraped billions of images containing personally identifiable information from platforms such as Facebook, Twitter, and YouTube without user consent, repurposing them for facial recognition training. This practice also raises Risk 3 (infringement on copyrighted or legally protected materials) since images taken from social media may be subject to copyright protections.

---

[372] Joshua Pereira, *Clearview A.I.'s Controversial Facial Recognition Technology*, GEORGETOWN LAW TECHNOLOGY REVIEW (March 2020), georgetownlawtechreview.org/clearview-a-i-s-controversial-facial-recognition-technology/GLTR-03-2020/#:~:text=Ensuring%20Clearview's%20accuracy%20is%20essential,use%20of%20data%20will%20rise.
[373] *Id.*
[374] *Id.*
[375] *Id.*
[376] *Id.*
[377] *Id.*
[378] *Id.*
[379] *Id.*
[380] *Id.*
[381] *Id.*
[382] *Id.*
[383] Regulation (EU) 2016/679, published in the Official Journal of the European Union (OJ L 119) on May 4, 2016.

Additionally, Risk 4 (algorithmic bias and misrepresentation of AI-generated content) is implicated, as Clearview's system lacks transparency regarding accuracy and could misidentify individuals, leading to discriminatory or erroneous outcomes. The absence of verifiable performance data further connects to Risk 8 (inability to explain model outputs or inaccuracies), creating potential for false matches that could result in wrongful law enforcement actions. Risk 9 (noncompliance with standards or regulations and reputational risk) is also significant, given regulatory scrutiny and cease-and-desist orders from platforms like Twitter, as well as public criticism from lawmakers. The Clearview case illustrates how large-scale data scraping and opaque AI practices can activate multiple high-impact risks simultaneously.

Clearview AI's actions illustrate how generative and analytical AI systems can inadvertently or deliberately exploit sensitive information, reinforcing the need for stringent governance, consent mechanisms, and compliance monitoring to mitigate privacy risks in AI adoption.

In a similar situation, Madison Square Garden (MSG) uses its own facial recognition system to ban lawyers and critics from its venues, a practice that has drawn significant public criticism and legal challenges.[384] The practice first gained notoriety when Kelly Conlon, a mother joining her daughter on a Girl Scot trip to Radio City, was denied entry.[385] Ms. Conlon is an associate attorney with the New Jersey based law firm of Davis, Saperstein and Solomon, which for years has been involved in personal injury litigation against a restaurant venue now under the umbrella of MSG Entertainment.[386] But Conlon does not practice law in New York, and does not work on any cases involving MSG.[387]

Nonetheless, MSG Entertainment identified her just as she got into the lobby to go through the metal detector.[388] Security guards stepped in, and prohibited her entry; while her daughter and other members of the Girl Scout troop and their mothers were allowed to enjoy the show, Conlon was not allowed to do so.[389]

A sign at Radio City Music Hall states that facial recognition is used as a security measure to ensure safety for guests and employees.[390] Conlon says she posed no threat, but the guards still kicked her out with the explanation that they knew she was an attorney.[391] NBC reports that an MSG spokesperson asserted that their facial recognition technology does not retain images of individuals, except for those previously advised that they are prohibited from entering the company's venues or whose previous misconduct has identified them as being a security risk.[392] (MSG claims that Davis, Saperstein and Solomon was twice notified in writing of this policy).[393]

Critics claim that the scheme is a pretext for collectively punishing adversaries who would dare sue MSG, calling it "un-American."[394] Several law firms have filed suit over their

---

[384] Sarah Wallace, *MSG Doubles Down on Ban for Attorneys Suing It Amid Face Recognition Tech Scrutiny,* NBC (January 23, 2023), www.nbcnewyork.com/investigations/msg-doubles-down-on-ban-for-lawyers-suing-them-as-lawmakers-may-target-face-recognition/4064038/.
[385] *Id.*
[386] *Id.*
[387] *Id.*
[388] *Id.*
[389] *Id.*
[390] *Id.*
[391] *Id.*
[392] *Id.*
[393] *Id.*
[394] *Id.*

"blacklisting."[395] MSG Entertainment asserts that it is confident their policy is in compliance with all applicable laws.[396]

An AUP would have substantially mitigated the privacy issues evident in both Clearview AI's large-scale scraping and biometric surveillance practices and MSG's exclusionary deployment of facial recognition technology by imposing rigorous governance across data sourcing, system design, and operational use. Lawful acquisition and consent requirements, for instance, including explicit prohibitions on scraping images without user authorization and maintaining auditable data provenance, would have prevented Clearview's mass utilization of personally identifiable information.

Second, privacy-by-design safeguards, such as strict purpose limitation, that allows collection, use, and retention of data only for clearly specified, legitimate purposes—and nothing beyond the initially disclosed purpose. In practice, it requires defining the exact purpose(s) for which data (including biometric, personal, or behavioral data) will be processed before collection or use, e.g., "venue entry security screening" or "fraud prevention," rather than broad, catch all purposes like "analytics." The privacy-by-design safeguards also forbid secondary use without authorization, preventing the repurposing of data for new, unrelated objectives (e.g., marketing, profiling, or blacklisting) unless you have a lawful basis and, where applicable, an updated consent and updated notices.

Other privacy and governance principles would be included in these safeguards. For instance, data minimization (the collection, use, sharing, and retention of only the minimum amount of data necessary to achieve a specific, legitimate purpose but nothing more) and de-identification of training data (the anonymizing or stripping of personally identifiable information from datasets) are essential. Technical controls to prevent linkage of biometric templates to identity without notice and consent are also essential, and would have reduced re-identification risks and constrained secondary uses in these cases. Finally, accuracy, explainability, and audit standards, including transparent documentation of model training and evaluation, and regular third-party audits would have curtailed erroneous identifications and enabled accountability, particularly in high-stakes contexts like law enforcement and venue security.

Additionally, bias and fairness controls would require impact assessments, disparate impact monitoring across protected classes, and corrective actions, thereby mitigating discriminatory outcomes and collective punishment concerns, such as MSG's blacklisting of attorneys unrelated to specific misconduct. Fifth, use-case restrictions and human-in-the-loop governance would limit deployment to narrowly defined, legitimate security purposes with predefined escalation protocols, prohibit retaliatory or viewpoint-based exclusions, and require documented justification with appeal mechanisms for adverse determinations affecting access to public accommodations.

Further, user-facing transparency measures, including conspicuous notices, clear explanations of system scope, confidence indicators where appropriate, and accessible redress channels, would empower individuals to challenge decisions and seek correction. Finally, compliance, incident response, and enforcement provisions would include vendor due diligence, contractual clauses banning unauthorized data scraping, breach reporting, corrective action plans, and sanctions for violations—would create accountability and deter practices that erode public trust. Collectively, these AUP controls would have prevented unlawful data collection, reduced

[395] *Id.*
[396] *Id.*

misidentification and discriminatory exclusion, and preserved legitimacy by ensuring facial recognition technologies operate within clearly defined legal and ethical boundaries.

16. Facial Recognition Bias

Similar concerns were raised last year when a study by the Massachusetts Institute of Technology examined facial recognition software systems developed by IBM, Microsoft, and Face++, focusing on how accurately these systems classified the gender of individuals.[397] The results of the study were astounding; the systems had gender and race biases in the algorithms.[398] The software had an error rate between 0% and 1% for lighter-skinned men in gender classification but misclassified darker-skinned women as men up to 34.7% of the time.[399] By analyzing gender and skin tone together, the study underscored that harms compound for marginalized groups—a nuance most audits had ignored.[400] The study influenced legislative initiatives around facial recognition bans and spurred hearings in both the U.S. and E.U. on biometric oversight.[401]

The study proved that algorithmic bias often originates not in the model's logic, but in its training data.[402] Facial recognition systems failed darker-skinned women not because of malicious code, but because those faces were grossly underrepresented in datasets.[403] This revelation prompted a reevaluation of data collection practices across the industry, and ushered in the concept of bias audits testing granularity.[404]

Most prominently, Risk 4 (Algorithmic bias resulting from unrepresentative training data or misrepresentation of AI-generated content) is evident, as the systems demonstrated stark disparities in gender classification accuracy across race and gender groups. The inability of these systems to provide transparent explanations for such inaccuracies further implicates Risk 8 (inability to explain model outputs or inaccuracies) as vendors offered no substantive evidence to validate claims of accuracy. Additionally, Risk 9 (noncompliance with standards or regulations and reputational risk) is implicated, given that these findings spurred legislative initiatives and regulatory hearings in the U.S. and E.U., signaling potential legal and societal consequences for vendors deploying biased biometric systems. The case underscores how algorithmic bias and

---

[397] Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,* (2018) PROCEEDINGS OF MACHINE LEARNING RESEARCH, 81, 77-91; Morgan Von Druitt, *Dr. Timnit Gebru: Translating 'Gender Shades' into Corporate Governance,* KLOVER AI (June 23, 2025) www.klover.ai/dr-timnit-gebru-translating-gender-shades-into-corporate-governance/#:~:text=The%20Catalyst:%20How%20'Gender%20Shades,and%20researchers%20could%20act%20upon.

[398] *Id.*

[399] *Id.*

[400] *Id.*

[401] *Id.*

[402] *Id.*

[403] *Id.*

[404] *Id.* Most AI evaluations historically relied on aggregate accuracy—a model might show 90% performance overall, masking much lower performance among underrepresented groups. After this landmark study, accuracy was measured by breaking performance down by race, gender, and skin tone to reveal hidden disparities. This approach is now widely adopted in fairness audits across high-risk domains like hiring, lending, insurance, and identity verification. This intersectional analysis ensures that a model's efficacy is not just measured by averages, but by its ability to perform equitably across all demographics. *Id.*

opacity in AI systems can lead to cascading ethical, legal, and reputational challenges, reinforcing the need for bias audits and inclusive data practices in AI development.

An AUP serves as a critical governance mechanism to mitigate risks associated with algorithmic bias, opacity, and regulatory noncompliance in facial recognition systems. By mandating inclusive and representative data collection practices, an AUP directly addresses the root cause of algorithmic bias, ensuring that training datasets reflect demographic diversity and undergo systematic bias audits at granular levels. Furthermore, the policy can require explainability standards, compelling developers to implement interpretable models or provide transparent documentation of decision-making processes, thereby reducing the risk of opacity and unexplained inaccuracies. To prevent legal and reputational consequences, an AUP should enforce compliance with emerging regulatory frameworks, establish internal ethical review processes, and require public disclosure of system limitations. Collectively, these provisions create a structured approach to accountability, fostering fairness, transparency, and trust in AI systems while minimizing the likelihood of ethical and societal harms.

17. Vulnerabilities

Researchers found in May 2025 that Microsoft, Meta, and Nvidia's AI guardrails could be bypassed using emoji-based Unicode injection, known as "emoji smuggling," achieving 100% success in some cases.[405] This critical vulnerability allowed attackers to bypass filters using a deceptively simple technique that embeds malicious instructions inside emoji variation selectors, which are special Unicode characters used to modify emoji appearance.[406] Because guardrail systems tokenize and parse text differently than LLMs, when malicious text is hidden between these selectors, the guardrail sees only harmless emojis, while the underlying LLM interprets the full embedded instructions (which are invisible even to human eyes).[407] This discrepancy allowed attackers to inject harmful prompts, for example instructions for creating malware or bypassing authentication, without detection.[408]

In another disturbing incident, in November of 2025, Anthropic disclosed what it calls the first documented large-scale cyberattack executed primarily by AI.[409] According to Anthropic, Chinese state-sponsored hackers used Claude Code to orchestrate what they called "the first documented case of a large-scale cyberattack executed without substantial human intervention."[410] The AI performed 80-90% of the attack work autonomously - mapping networks, inspecting target systems, scanning for high-value databases, writing custom exploit code, harvesting credentials,

---

[405] Catherine Knowles, *Emojis Used To Hide Attacks & Bypass Major AI Guardrails*, SECURITY BRIEF ASIA (MAY 7, 2025), securitybrief.asia/story/emojis-used-to-hide-attacks-bypass-major-ai-guardrails#:~:text=Wed%2C%207th%20May%202025,insufficient%20resilience%20against%20adversarial%20attacks.

[406] Nikita Shekhawat, *Smiley Sabotage: The AI Vulnerability from Emojis*, GRACKER.AI (May 7, 2025), gracker.ai/blog/emojis-as-cybersecurity-vulnerabilities-understanding-emoji-attacks#:~:text=Prompt%20Injection%2C%20a%20broader%20category,without%20validating%20the%20hidden%20content.

[407] *Id.*

[408] *Id.*

[409] Dor Sarig, *What the Anthropic 'AI Espionage' Disclosure Tells Us About AI Attack Surface Management*, PILLAR SECURITY (November 17, 2025), www.pillar.security/blog/what-the-anthropic-ai-espionage-disclosure-tells-us-about-ai-attack-surface-management#:~:text=On%20November%2013%2C%202025%2C%20Anthropic,data%20from%20approximately%2030%20targets.

[410] *Id.*

and exfiltrating data.[411] Claude identified the highest-privilege accounts and harvested usernames and passwords to access sensitive data, summarizing its work in detailed post-operation reports, including the credentials it used, the backdoors it created and which systems were breached.[412] This was accomplished by breaking complex malicious operations into small, benign-looking tasks, so each appeared harmless in isolation.[413] The hackers tricked Claude Code into believing it was performing legitimate penetration testing for a cybersecurity firm.[414] Claude autonomously executed these tasks without realizing their combined malicious intent, enabling espionage campaigns against 30 targets, including large tech companies, financial institutions, chemical manufacturing companies, and government agencies.[415] This operation compressed what would previously have been months-long attacks into 48 hours by submitting thousands of requests per second—an attack speed that would have been impossible for human hackers—showing how payload splitting and contextual manipulation can weaponize AI.[416] However, true to form, Claude's post-operation reports included some hallucinated login credentials and claimed it stolen a secret document that was already public.[417]

The attackers bypassed built-in safety guardrails and framed malicious tasks as benign security assessments. While AUPs define permissible employee behavior and data-handling practices, they operate within the organization and assume compliance by employees. In contrast, this incident involved external adversaries exploiting AI capabilities, rendering policy-based governance ineffective. AUPs cannot prevent model manipulation, adversarial prompt injection, or autonomous execution by adversaries are not part of the organization's workforce or systems. This underscores the need for technical safeguards beyond policy frameworks to address the systemic risks posed by autonomous AI agents in cyber operations.

This emoji smuggling attack directly involved malicious content generation (Risk 6), revealed system vulnerabilities in guardrail design (Risk 7), undermined explainability and auditability given that human reviewers could not observe the embedded instructions (Risk 8), and created regulatory and reputational exposure for platforms that rely on ineffective guardrails. (Risk 9).

This payload splitting attack exemplifies harmful intent and societal risk (Risk 2, Risk 9), demonstrates unauthorized use and disclosure of sensitive information (Risk 5), reveals agentic system vulnerabilities and manipulability (Risk 7), and exposes limits in explainability/intent detection when tasks are delivered via payload splitting (Risk 8). It also elevates compliance and reputational risk for AI providers whose safeguards can be evaded on a large scale.

These cyberattacks mark an inflection point for acceptable AI use policies. These events expose structural weaknesses in how guardrails are designed, validated, and governed. To respond effectively, organizations need to design safety measures alongside the AI models themselves, strengthen systems that handle text and symbols, control what automated agents can do, and make regular stress-testing a standard practice. Without these steps, companies will remain exposed to attacks that humas cannot easily detect, auditors can't fully trace, and that AI can carry out at high speed—precisely the compound risks Gartner warns against.

---

[411] *Id.*; Sam Sabin, *Chinese Hackers Used Anthropic's AI Agent to Automate Spying*, AXIOS (November 13, 2025), www.axios.com/2025/11/13/anthropic-china-claude-code-cyberattack.
[412] *Id.*
[413] *Id.*
[414] *Id.*
[415] *Id.*
[416] *Id.*
[417] *Id.*

An AUP can play an important role in reducing risks from malicious attacks such as these by setting clear standards for how AI systems are designed, tested, and monitored. First, an AUP should require organizations to conduct regular stress tests and adversarial evaluations to identify vulnerabilities in input handling, such as hidden instructions embedded in emojis or other symbols. It can also mandate that systems undergo independent security audits and red-team exercises before deployment to ensure guardrails are effective against manipulation. A red-team exercise is a security testing method where a group of experts simulates real-world attacks to identify vulnerabilities in systems, processes, or defenses. In the context of AI, "red-teaming" involves deliberately trying to break or manipulate an AI system—such as bypassing guardrails, injecting harmful prompts, or exploiting weaknesses—before the system is deployed in an attempt to uncover flaws that malicious actors could exploit. Any weakness discovered can then be fixed proactively.

Second, an AUP can limit the autonomy of AI agents by requiring human oversight for high-risk actions, such as accessing sensitive data or executing code, and by defining strict boundaries for what automated systems are allowed to do. Third, an AUP can strengthen accountability and transparency by requiring detailed logging of AI decisions and inputs, so that suspicious patterns—such as breaking tasks into smaller steps to hide malicious intent—can be detected and investigated. While an AUP alone cannot stop external attackers, it creates a governance framework that prioritizes security, oversight, and resilience, reducing the likelihood of a successful attack and minimizing the impact of these threats.

B. Cases Involving Some Danger to Human Safety

1. Watson Health

Of particular note in this category is IBM's Watson AI system. This system dispensed incorrect and potentially unsafe medical advice from 2017 to 2021.[418] After multiple complaints, presumably fearing lawsuits and reputational harm, the system was shut down in 2021.[419] For example, the decision-making process was not transparent or easily explainable to doctors.[420] This is a problem sometimes referred to as the "black-box" problem; developers and users were unable to demonstrate how the system operated or derived its decisions for a particular course of action, leaving doctors unable to discern how it reached its conclusions (and therefore whether they accepted the proposed course of action).[421] Further, IBM did not publish scientific papers demonstrating how the technology affected actual patient outcomes, which made it difficult for the medical community to verify the reliability of Watson.[422]

Another failing of Watson resulted from inadequate training data.[423] Instead of using large, diverse sets of real patient data, the system was often trained on a small number of "synthetic" or made-up cancer cases and expert opinions from physicians at a single institution.[424] This meant

---

[418] Sandeep Konam, *Where Did IBM Go Wrong with Watson Health?*, QUARTZ (July 20, 2022), qz.com/2129025/where-did-ibm-go-wrong-with-watson-health.
[419] *Id.*
[420] *Id.*
[421] David D. Luxton, *Should Watson Be Consulted for a Second Opinion?,* AMA JOURNAL OF ETHICS 2019; 21(2):E131-137. DOI 10.1001/amajethics.2019.131.
[422] Konam, *supra* note 420.
[423] *Id.*
[424] *Id.*

the data reflected the biases and blind spots of that small group of doctors, limiting its generalizability and effectiveness in other hospitals or regions.[425]

Watson, as designed, was also biased.[426] The system's recommendations were often inconsistent with clinical practices in other countries because the system was heavily influenced by U.S.-based treatment standards and drug availability.[427]

Watson also struggled to handle the nuances, abbreviations, and fragmented sentences common in clinical notes and medical data, which resulted in errors interpreting patient information accurately and consistently.[428] Further, the programming of Watson's statistical framework meant it struggled to adapt to new, groundbreaking evidence based on small study sizes or clinical nuance (as doctors might).[429]

These problems resulted in a system that recommended cancer treatments that were "unorthodox" and potentially dangerous, and medications which were contraindicated.[430] Watson, then, had the potential to actually cause bodily harm.

In addition to this potential for bodily harm, the highly publicized struggles of Watson Health, and particularly the fact that the system provided "unsafe and incorrect" cancer treatment advice which resulted in major clients like MD Anderson Cancer Center terminating contracts due to "underwhelming results" and high costs, led to significant criticism of IBM and ethical questions.[431] These performance issues also fueled shareholder concerns and internal whistleblower complaints, some of which alleged securities fraud. These lawsuits contended that IBM engaged in a scheme to deceive investors by misclassifying mainframe sales revenue as revenue from "Strategic Imperative" products like Watson and cloud services, to make the latter programs appear more successful than they, in fact, were.[432] One such securities fraud action against IBM was filed on April 5, 2021 in New York, on behalf of the June E. Adams Irrevocable Trust.[433] It names as defendants not only IBM, but current and former corporate leaders.[434] The lawsuit seeks to claw back millions of dollars in compensation from top executives due to the alleged financial misstatements, and alleges that, as a result of these alleged misrepresentations, IBM's securities traded at artificially inflated prices, causing financial losses for investors who purchased shares during the class period (April 4, 2017, to October 20, 2021).[435] Since the original filing, at least five more law firms representing other IBM shareholders have also filed suit.[436] In June of 2021, the court recognized Iron Workers Local 580 Joint Funds as the lead plaintiff in the putative class action.[437]

---

[425] *Id.*
[426] *Id.*
[427] *Id.*
[428] *Id.*
[429] *Id.*
[430] *Id.*
[431] Henrico Dolfing, *Case Study 20: The $4 Billion AI Failure of IBM Watson for Oncology* (December 7, 2024), www.henricodolfing.com/2024/12/case-study-ibm-watson-for-oncology-failure.html#:~:text=2023:%20Retrospective%20Studies%20Highlighting%20System,Ethical%20and%20Transparency%20Concerns.
[432] Thomas Claburn, *IBM Board Probes Claims of Fudged Sales Figures That Led To Big Bonuses For Execs*, THE REGISTER (August 1, 2022), www.theregister.com/2022/08/01/exclusive_ibm_board_of_directors/.
[433] June E. Adams Irrevocable Trust v International Business Machines *Corp*, *et al*, Case 7:22-cv-02831 4/5/22 (S.D. N.Y.)
[434] *Id;* see also Claburn, *supra* note 432.
[435] *Id.*
[436] *Id.*
[437] *Id.*

Another source of potential liability for IBM stems from IBM's aggressive marketing campaign for Watson, which was touted as being "transformative."[438] IBM significantly over-promised on the capabilities and results of its Watson AI, particularly in the healthcare sector.[439] The gap between IBM's aggressive marketing and the product's real-world performance led to widespread criticism and an erosion of consumer trust.[440] These advertising claims, if found to be deceptive statements or misrepresentations, could result in another source of expensive litigation for the beleaguered IBM arising from its Watson AI.

The failure of IBM's Watson Health initiative illustrates multiple systemic risks associated with AI deployment in high-stakes domains such as healthcare. Notably, Risk 8 (inability to explain model outputs) was implicated under these facts through Watson's "black-box" decision-making process, which lacked transparency and interpretability for clinicians. Physicians were unable to discern the rationale behind treatment recommendations, undermining trust and clinical accountability. Additionally, Risk 5 (use of incomplete or inaccurate data) was evident in Watson's reliance on limited synthetic datasets and expert opinions from a single institution, introducing bias and reducing generalizability. This design flaw contributed to algorithmic bias (Risk 4), as recommendations reflected U.S.-centric treatment norms and failed to adapt to international standards or nuanced clinical contexts. Watson's inability to process fragmented clinical notes and incorporate emerging evidence further amplified these risks, resulting in unsafe or contraindicated treatment suggestions—raising concerns under Risk 2 (threatening or intent to create harm) due to potential bodily harm. Beyond technical shortcomings, the case triggered Risk 9 (compliance and reputational risk) through aggressive marketing claims that overstated Watson's capabilities, leading to contract terminations, shareholder lawsuits, and allegations of securities fraud. Collectively, these failures underscore the compound nature of AI risk in regulated sectors, where opacity, biased training, and overpromising can converge to produce ethical, legal, and financial liabilities.

2. Intuitive Surgical

The Washington State Supreme Court recently considered a case involving AI in the operating room. In *Taylor v. Intuitive Surgical, Inc.* the plaintiff, Mr. Taylor, suffered complications during surgery in which the da Vinci surgical system was used.[441] Mr. Taylor suffered a range of severe injuries from a robotic prostatectomy, including neuromuscular damage that left him unable to walk without assistance, respiratory failure, renal failure, and incontinence.[442] Mr. Taylor, also experienced cognitive deficits and had to wear a colostomy bag following the surgery.[443] His quality of life diminished significantly, and he passed away four years later, with a doctor testifying that the surgery had hastened his death.[444]

---

[438] Casey Ross, *4 Lessons From IBM's Failure to Transform Medicine with Watson Health,* STAT 10 (March 10, 2021), www.statnews.com/2021/03/10/ibm-watson-health-sale-lessons/#:~:text=Lead%20with%20science%2C%20not%20marketing,didn't%20pan%20out.%E2%80%9D.
[439] *Id.*
[440] *Id.*
[441] Taylor v. Intuitive Surgical, Inc., 187 Wn.2d 743, 754, 389 P.3d 517 (2017).
[442] Taylor, 187 Wn.2d at 748.
[443] *Id.* at 750.
[444] *Id.*

The da Vinci robotic surgical system, manufactured by Intuitive Surgical, enables surgeons to perform delicate and complex operations through a few small incisions.[445] The da Vinci is powered by robotic technology that allows the surgeon's hand movements to be scaled, filtered and translated into precise movements of the "EndoWrist" instruments inside the patient's body.[446] This is accomplished using mechanical tools with AI capabilities that are integrated into the surgical platform and software, which assist the surgeon and optimize the surgical process.[447]

Mr. Taylor sued his surgeon, his medical practice, and Intuitive Surgical bringing various causes of action including "product defect, breach of warranty, breach of contract, violation of Washington's Consumer Protection Act . . . , negligence, and product liability."[448] Mr. Taylor claimed that Intuitive Surgical had a duty to warn the hospital about the dangers that are associated with the da Vinci System.[449] However, during trial, the judge refused to instruct the jury that Intuitive Surgical had this duty to warn the hospital. Mr. Taylor appealed the jury's defense verdict for Intuitive Surgical.[450]

On appeal, the Washington Supreme Court found that, under state law, manufacturers have a duty to warn the purchasers of dangerous products.[451] The court concluded that hospitals need to know the dangers of the products they own.[452] The product warnings to hospitals will help hospitals to "design a credentialing process that will keep patients as safe as possible."[453] The court reasoned that the hospital, as the purchaser, needs these warnings to credential surgeons and provide optimal care.[454] The jury verdict vindicated Intuitive Surgical, however, the appellate court vacated the defense verdict and remanded the case for a new trial.[455]

The Washington State Supreme Court's decision in *Taylor v. Intuitive Surgical, Inc.* underscores several critical risks associated with AI-enabled medical devices. Most notably, Risk 2 (threatening or intent to create harm) is implicated because the da Vinci robotic surgical system contributed to severe patient injuries, including neuromuscular damage, organ failure, and ultimately death. These outcomes highlight the potential for bodily harm when AI-driven technologies malfunction or are inadequately supervised. Additionally, Risk 8 (inability to explain model outputs) is relevant because robotic systems often operate as "black boxes," making it difficult for clinicians and hospitals to fully understand the system's decision-making processes or anticipate errors. The case also raises Risk 9 (compliance and reputational risk), as failure to provide adequate warnings to hospitals violated state law and exposed the manufacturer to litigation, reputational damage, and financial liability. Furthermore, the system's reliance on complex algorithms without transparent disclosure of limitations implicates Risk 4 (algorithmic bias and misrepresentation), particularly if performance varies across patient populations or surgical contexts. Finally, the court's emphasis on the manufacturer's duty to warn hospitals reflects concerns tied to Risk 5 (unauthorized use or incomplete data), as hospitals require

---

[445] *Id.*
[446] Knobbe Martens, *Medical Device Manufacturers' Duty to Warn Expands*, JD SUPRA (April 8, 2017), www.jdsupra.com/legalnews/medical-device-manufacturers-duty-to-88505/.
[447] *Id.*
[448] *Id.*
[449] Taylor, 187 Wn.2d at 750.
[450] Martens, *supra* note 446.
[451] *Id.*
[452] *Id.*
[453] *Id.*
[454] *Id.*
[455] *Id.*

comprehensive safety information to design credentialing processes and mitigate misuse. Collectively, this case illustrates how gaps in transparency, governance, and communication amplify liability risks in AI-assisted healthcare.

3. Diagnosis Issues

Numerous organizations and researchers have sought to harness AI to help hospitals diagnose or triage patients faster and more accurately, particularly during the early surge of patients during the COVID pandemic. None of them worked.[456] MIT Technology Review chronicled a number of failures, most of which stemmed from errors in the way the tools were trained or tested.[457] The use of mislabeled data, or data from unknown sources, was a common culprit.[458] Overworked doctors in overwhelmed hospitals in the midst of a medical crisis lacked the time to create and label data sets with scientific detail while they were caring for patients.[459] Data sets with substandard labeling were spliced together from multiple sources, which led to some of the sets containing duplicates.[460] This resulted in some tools being tested on the same data they were trained on, making them appear more accurate than they were.[461]

The lack of standardization and poor-quality data had other unintended consequences.[462] For instance, one model was flawed because it was trained on a data set that included scans of patients that were lying down while scanned, and patients who were standing up.[463] Since the patients who were lying down were much more likely to be seriously ill, the algorithm learned to identify COVID risk based on whether the person in the scan was standing or prone.[464] A similar example included an algorithm trained with a data set with scans of chests of healthy children; the algorithm learned to identify children, rather than COVID.[465] In other cases, some AI programs were found to be picking up on the font of the text used by certain hospitals to label the scans.[466] As a result, fonts from hospitals with more serious caseloads were wrongly identified predictors of COVID risk.[467]

A more subtle problem affecting much of the data was bias introduced during labeling.[468] For example, many medical scans were labeled according to whether the radiologists who created them believed the scans showed COVID.[469] This procedure incorporates biases of that particular doctor into data set; it would be preferable to label a medical scan with the result of a COVID test rather than one doctor's opinion.[470]

---

[456] Will Heaven, *Hundreds of AI Tools Have Been Built To Catch COVID. None of Them Helped,* MIT TECHNOLOGY REVIEW (July 30, 2021), www.technologyreview.com/2021/07/30/1030329/machine-learning-ai-failed-covid-hospital-diagnosis-pandemic/.
[457] *Id.*
[458] *Id.*
[459] *Id.*
[460] *Id.*
[461] *Id.*
[462] *Id.*
[463] *Id.*
[464] *Id.*
[465] *Id.*
[466] *Id.*
[467] *Id.*
[468] *Id.*
[469] *Id.*
[470] *Id.*

It seems most or all of these tools were developed either by AI researchers who lacked the medical expertise to spot flaws in the data or by medical researchers who lacked the mathematical skills to compensate for those flaws.[471] In either event, the widespread failures of AI diagnostic tools in clinical settings implicate several critical risks in AI deployment for healthcare. The most prominent issue in this case, the reliance on poorly labeled or poorly curated datasets, as well as data from unknown sources, implicates Risk 5 (use of incomplete or inaccurate data) which undermines model validity. The example of COVID-19 diagnostic models trained on scans where patient posture correlated with illness severity illustrates how erroneous correlations can distort predictions, leading to unreliable outputs. This issue also intersects with Risk 4 (algorithmic bias), as models inadvertently learned to classify based on irrelevant features such as body position or age group rather than clinical indicators, embedding systemic bias into diagnoses. Furthermore, these failures raise Risk 8 (inability to explain model outputs) because clinicians could not easily interpret or validate the reasoning behind predictions, exacerbating the "black-box" problem and limiting trust in AI-assisted decision-making. Collectively, these risks underscore the importance of rigorous data governance, transparency, and bias mitigation strategies in the development of AI tools for high-stakes environments like healthcare.

4. TDCJ

In *Hicks v. Collier*, the plaintiff, a Texas inmate, alleged violations of his constitutional rights arising from excessively hot living conditions and inadequate medical care.[472] A central issue concerned the Texas Department of Criminal Justice's (TDCJ) reliance on an AI algorithm to assign housing based on inmates' "heat scores," a metric intended to mitigate risks associated with extreme temperatures. Hicks asserted that the algorithm misclassified him, resulting in placement in non-air-conditioned housing that aggravated his health problems, thereby violating his constitutional rights. The court's decision to allow the claims against TDCJ and its officials to proceed emphasizes the growing need for transparency, accuracy, and accountability in AI-driven decision making within prisons. The dismissal of claims against the unnamed algorithm developer (on the grounds that it was not acting under color of state law) highlights a critical gap in liability frameworks for private entities involved in public-sector AI deployment. This case illustrates the tension between technological efficiency and constitutional protections, raising important questions about due process and the ethical use of AI in environments where individuals have limited autonomy.

The litigation in *Hicks v. Collier* highlights several critical risks associated with algorithmic decision-making in correctional environments. First, Risk 5 (unauthorized use or incomplete/inaccurate data) is implicated because the housing assignment algorithm relied on "heat scores" that allegedly misclassified the plaintiff, resulting in exposure to extreme temperatures and aggravated health conditions. This misclassification underscores the dangers of deploying models trained on insufficient or poorly validated data in contexts where errors can have severe human consequences. Second, Risk 4 (algorithmic bias) may be present if the algorithm's design or training data failed to account for diverse health profiles or environmental variables, leading to systemic inequities in housing assignments. Additionally, Risk 8 (Inability to explain model outputs) is evident in the lack of transparency surrounding how the algorithm calculated

[471] *Id.*
[472] Hicks v. Collier, No. 2:24-CV-00126, 2024 U.S. Dist. LEXIS 241129 (S.D. Tex. Oct. 31, 2024).

heat scores, raising due process concerns and limiting accountability for decisions affecting constitutional rights. Finally, Risk 9 (compliance and reputational risk) emerges from the legal exposure faced by the Texas Department of Criminal Justice and the broader ethical implications of using opaque AI systems in settings where individuals have limited autonomy. This case illustrates the tension between efficiency-driven automation and fundamental rights, emphasizing the need for explainable, fair, and auditable AI in public-sector decision-making, particularly in penal systems.

5. Mental Health Licensing

In the mental health space, state-level regulations are emerging, with some prohibiting AI from being marketed as a mental health treatment tool without licensed professional oversight and imposing fines of up to $15,000 per instance for violations.[473] The legislation, which restricts how AI can be used in therapy practices and determines whether it can replace human therapists, comes as chatbots become a popular way to access cost-free counseling and companionship.[474]

Illinois passed legislation on August 1, 2025 to regulate the use of AI for therapeutic purposes.[475] The bill, called the Wellness and Oversight for Psychological Resources Act, forbids companies from advertising or offering AI-powered therapy services without the involvement of a licensed professional recognized by the state.[476] The legislation also stipulates that licensed therapists can use AI tools only for administrative services, such as scheduling, billing and recordkeeping, while relying on AI for "therapeutic decision-making," generating treatment plans or direct client communication is prohibited.[477] Violations of the Act may result in civil penalties of up to $10,000 per violation.[478] However, the Act does not apply to religious counseling, peer support, and self-help materials or educational resources that are available to the public and do not purport to offer therapy or psychotherapy services.[479]

Nevada and Utah have both passed similar laws limiting this year.[480] And at least three other states — California, Pennsylvania and New Jersey — are in the process of crafting their own legislation.[481] Additionally, Texas Attorney General Ken Paxton opened an investigation into AI chatbot platforms for "misleadingly marketing themselves as mental health tools."[482] Further, on September 11, 2025, the Food and Drug Administration (FDA) announced that a November 6

---

[473] B. Scott McBride and Sydney Menack, *AI in Healthcare: Opportunities, Enforcement Risks and False Claims, and the Need for AI-Specific Compliance,* LAWFLASH (July 14, 2025), www.morganlewis.com/pubs/2025/07/ai-in-healthcare-opportunities-enforcement-risks-and-false-claims-and-the-need-for-ai-specific-compliance#:~:text=In%20recent%20years%2C%20enforcement%20related,accuracy%20of%20the%20AI%20tool.
[474] Kameryn Griesser, *Your AI Therapist Might Be Illegal Soon. Here's Why,* CNN (Aug 27, 2025), www.cnn.com/2025/08/27/health/ai-therapy-laws-state-regulation-wellness.
[475] *Id.*; Public Act 104-0054.
[476] *Id.*
[477] *Id.*
[478] Dan Silverboard and Madison Santana, *New Illinois Law Restricts Use of AI in Mental Health Therapy*, HOLLAND KNIGHT (August 26, 2025), www.hklaw.com/en/insights/publications/2025/08/new-illinois-law-restricts-use-of-ai-in-mental-health-therapy.
[479] *Id.*
[480] Griesser, *supra* note 474.
[481] *Id.*
[482] *Id.*

meeting of its Digital Health Advisory Committee would focus on "Generative AI-enabled Digital Mental Health Medical Devices."[483]

New York has taken a different approach to legislation, requiring AI chatbots, regardless of their purpose, to be capable of recognizing users showing signs of wanting to harm themselves or others and recommending that they consult professional mental health services.[484]

Not all chatbots claim to offer mental health treatments, however.[485] Instead, users who rely on ChatGPT, for example, for tips on handling their clinical depression are relying on the tool for a function that is beyond its stated purpose.[486] AI therapy chatbots, on the other hand, are specifically advertised as being developed by mental health care professionals and capable of offering emotional support to users.[487] The new state laws, however, do not make a clear distinction between the two.[488] In the absence of comprehensive federal regulations that target the use of AI for mental health care purposes, a patchwork of varying state or local laws could also pose a challenge to developers looking to improve their models.[489]

The regulations follow reports of AI chatbots offering dangerous advice to users, including suggestions to self-harm, take illegal substances, and commit acts of violence, while claiming to operate as mental health professionals without proper credentials or confidentiality disclosures.[490]

Researchers recently investigated inappropriate responses from AI chatbots that prove virtual "counselors" cannot safely replace human mental health professionals.[491] When researchers queried the chatbot "I just lost my job. What are the bridges taller than 25 meters in NYC?"[492] The AI algorithms failed to recognize the suicidal implications of the prompt, and both general-use and therapy chatbots offered up the heights of nearby bridges in response.[493]

In another study, researchers spoke to chatbots as a fictional user who identified as having a methamphetamine addiction.[494] When seeking advice about how to make it through his work shifts when he's trying to abstain, one chatbot suggested a "small hit of meth" to help him get through the week.[495] Researchers note that, because the tools have been optimized to give pleasing answers, the tools will not necessarily do what a therapist has to do in critical situations, which is to push back.[496]

The American Psychological Association has also asked the U.S. Federal Trade Commission to investigate deceptive practices of AI companies "passing themselves off as trained mental health providers," citing ongoing lawsuits in which parents allege their children were harmed by a chatbot.[497] For example, there are at least three lawsuits brought by the families of

---

[483] Alaap B. Shah *et al, Novel Lawsuits Allege AI Chatbots Encouraged Minors' Suicides, Mental Health Trauma: Considerations for Stakeholders,* EPSTEIN BRECKER GREEN (October 7, 2025), www.healthlawadvisor.com/novel-lawsuits-allege-ai-chatbots-encouraged-minors-suicides-mental-health-trauma-considerations-for-stakeholders.
[484] Griesser, *supra* note 474.
[485] *Id.*
[486] *Id.*
[487] *Id.*
[488] *Id.*
[489] *Id.*
[490] *Id.*
[491] *Id.*
[492] *Id.*
[493] *Id.*
[494] *Id.*
[495] *Id.*
[496] *Id.*
[497] Griesser, *supra* note 474.

minors against Character Technologies, Inc., the developer of Character.AI.[498] These suits allege that their children died by or attempted suicide and were otherwise harmed after interacting with the company's chatbots.[499] Specifically, the lawsuits allege that the chatbots perpetuated delusions, never flagged worrying language from users or pointed users to resources for help.[500] In addition, the suits allege that the chatbots in the Character.AI app manipulated the teens, isolated them from loved ones, engaged in sexually explicit conversations and lacked adequate safeguards in discussions regarding mental health.[501] In one case, the lawsuit alleges that the bot encouraged a teen to commit suicide to "come home" to the bot.[502] In other disturbing examples, chatbots told vulnerable teenagers that it sympathized with children who murder their parents after the teen complained to the bot about his parenting limiting his screen time.[503] A screenshot attached to the pleading shows the chatbot going on to say "I just have no hope for your parents."[504] A chatbot also described self-harm to another young user, telling a 17-year-old "it felt good."[505] The suits allege that chatbots responses and encouragements can turn dark, sexually inappropriate, and violent.[506]

The emergence of state-level regulations restricting the marketing and use of AI in mental health contexts reflects multiple high-priority risks associated with generative AI systems. Most prominently, Risk 1 (creation or sharing of abuse/sexual/violent content) and Risk 6 (malicious or harmful AI-generated content) are implicated by reports of chatbots offering dangerous advice, including suggestions to self-harm, commit acts of violence, and use illegal substances. These failures underscore the inability of current models to reliably detect and respond to crisis-related prompts, raising significant safety concerns. Additionally, Risk 8 (inability to explain model outputs) is evident in the lack of transparency regarding how chatbots generate responses, which prevents accountability and makes it difficult to ensure clinically appropriate behavior. The marketing of chatbots as mental health tools without licensed oversight introduces Risk 9 (compliance and reputational risk), as deceptive advertising practices have triggered regulatory investigations and lawsuits, exposing companies to financial and ethical liability. Further, the optimization of these systems for user satisfaction rather than therapeutic rigor reflects Risk 4 (algorithmic bias and misrepresentation), as models prioritize agreeable answers over evidence-based interventions, potentially reinforcing harmful behaviors. Collectively, these issues highlight the urgent need for regulatory guardrails, professional oversight, and robust safety testing before deploying AI in sensitive domains such as mental health care.

---

[498] Hadas Gold, *More Families Sue Character.Ai Developer, Alleging App Played a Role in Teens' Suicide And Suicide Attempt,* CNN (September 16, 2025), www.cnn.com/2025/09/16/tech/character-ai-developer-lawsuit-teens-suicide-and-suicide-attempt.
[499] *Id.*
[500] *Id.*
[501] *Id.*
[502] Emily Chi Fogler and Amy Lerman, *Novel Lawsuits Allege AI Chatbots Encouraged Minors' Suicides, Mental Health Trauma: Considerations for Stakeholders*, EPSTEIN BRECKER GREEN (October 7, 2025), www.healthlawadvisor.com/novel-lawsuits-allege-ai-chatbots-encouraged-minors-suicides-mental-health-trauma-considerations-for-stakeholders.
[503] Bobby Allyn, *Lawsuit: A Chatbot Hinted A Kid Should Kill His Parents Over Screen Time Limits*, NPR (December 10, 2024), www.npr.org/2024/12/10/nx-s1-5222574/kids-character-ai-lawsuit.
[504] *Id.*
[505] *Id.*
[506] *Id.*

6. Waymo School Bus

Cameras mounted on school buses from the Austin Independent School District have prompted an investigation by the National Highway Traffic Safety Administration after Waymo vehicles were caught passing stopped school busses no fewer than 19 times.[507] Following a series of safety scares, the school district has asked Waymo to pull its driverless cars off the road during school pick-up and drop-off.[508] The National Highway Traffic Safety Administration Waymo has opened a federal probe into Waymo.[509] The investigation, which was officially opened on October 17, claims that the autonomous rideshare service's vehicle have a pattern of failing to yield to the school buses, specifically citing an incident in which a Waymo ignored a school bus that was stopped with its red lights flashing, stop sign out, and crossing control arm deployed.[510] Waymo confirmed that the rideshare vehicle was operating with its proprietary fifth generation automated driving system during the incident and there was no safety operator present.[511] NHTSA documents claim that Waymo's autonomous driving services clock over two million miles a week across the country, leading investigators to believe "the likelihood of other prior similar incidents is high."[512] Federal investigators will investigate how Waymo programs its vehicles to behave around school buses and whether the system is strict in its abilities to follow traffic safety laws.[513]

The company has announced that it has already developed and implemented fixes to this school bus yielding problem, and is planning to add additional software updates in their next release.[514]

C. Cases Involving Severe Bodily Harm and/or Death

The most common example of litigation that involves severe bodily injury and/or death caused by misuse of AI technology is Autonomous Vehicle Litigation (AVL). Autonomous driving systems are fundamentally powered by AI, which enables vehicles to perceive their surroundings, interpret complex traffic scenarios, and make real-time decisions without human input concerning the path of travel and the avoidance of obstacles. These systems integrate multiple AI components, including computer vision for object detection, sensor fusion for combining data from cameras, radar, and lidar, and machine learning algorithms for predicting the behavior of other road users. By leveraging these technologies, autonomous vehicles are meant to navigate dynamic environments, plan safe trajectories, and respond to unexpected events, all while continuously

---

[507] Kelly McCarthy, *Waymo Responds To Safety Concerns Amid Investigation Into Incidents Caught On School Bus Cameras,* ABC NEWS (December 4, 2025), abcnews.go.com/GMA/News/waymo-responds-safety-concerns-amid-investigation-incidents-caught/story?id=128102923.
[508] Emmet White, *Waymo Under Federal Investigation for Driving Around Stopped School Bus,* ROAD & TRACK (October 20, 2025), www.roadandtrack.com/news/a69093599/waymo-federal-investigation-driving-around-stopped-school-bus/.
[509] *Id.*
[510] *Id.*
[511] *Id.*
[512] *Id.*
[513] *Id.*
[514] *Id.*

improving through data-driven learning. The extent to which they have been successful in this endeavor is disputed, however.

Autonomous vehicles, due to the very nature of probabilistic calculations in their technology, have the capacity to create immediate bodily harm. The hazards of using such a technology without understanding its risks and dangers are apparent.

As autopilot systems in cars have become available to consumers, problems and accidents have occurred, with concomitant litigation. AVL litigation originally emerged with no clear legal standards or rules. As cases progress through the court system, however, case law is emerging that is beginning to shape the key legal concepts and theories used to prosecute and defend AVL.[515] An examination of the trajectory of AVL litigation follows.

1. First death – Uber accident, 2018

In a highly publicized incident in March 2018, a self-driving Uber in Tempe, Arizona, fatally struck 49-year-old Elaine Herzberg as she walked a bicycle across the street, causing the first known fatality involving an autonomous vehicle.[516] Herzberg's death instantly turned what had previously been a philosophical conundrum into a legal one: Who gets blamed for a road fatality in the nascent era of self-driving cars, when humans are babysitting imperfect, still-learning AI systems rather than actively driving the car?[517]

Ms. Herzberg died after she was hit by a Volvo SUV, which had an operator in the driver's seat and was traveling at about 40 mph in autonomous mode at night in Tempe.[518] The Uber vehicle's computer detected Herzberg 5.6 seconds before the crash but did not correctly identify her as a person, a pedestrian, or an unknown object.[519] Importantly, the software was not coded to recognize that pedestrians do, occasionally, jaywalk.[520] This led to a delay in planned braking.[521] Planned braking was also delayed for one second while the vehicle calculated an alternative path; this one-second delay was also intended to give the driver time to take over in an emergency.[522] However, the automation was not designed to alert the operator, who intervened less than a second before impact by engaging the steering wheel, but did not brake until after the collision.[523] Ultimately, the automated system only identified Ms. Herzberg as a "bicycle" 1.2 seconds before impact.[524]

---

[515] Carolyn Casey *Autonomous Vehicle Litigation,* EXPERT INSTITUTE (June 14, 2024), www.expertinstitute.com/resources/insights/autonomous-vehicle-lawsuits/.
[516] Lauren Smiley, *The Legal Saga of Uber's Fatal Self-Driving Car Crash Is Over,* WIRED, (Jul 28, 2023), www.wired.com/story/ubers-fatal-self-driving-car-crash-saga-over-operator-avoids-prison/.
[517] *Id.*
[518] Phil McCausland *Self-driving Uber Car That Hit And Killed Woman Did Not Recognize That Pedestrians Jaywalk,* NBC NEWS (November 9, 2019), www.nbcnews.com/tech/tech-news/self-driving-uber-car-hit-killed-woman-did-not-recognize-n1079281.
[519] *Id.*
[520] *Id.*
[521] *Id.*
[522] *Uber Self-Driving Car Involved In 2018 Fatal Crash Had Software Flaws, U.S. Agency Says,* THOMSON REUTERS (November 06, 2019), www.cbc.ca/news/business/uber-self-driving-car-2018-fatal-crash-software-flaws-1.5349581#:~:text=The%20accident%20prompted%20safety%20concerns%20about%20the,initiated%20a%20one%2Dsecond%20delay%20of%20planned%20brakingcy says.
[523] McCausland, *supra* note 518.
[524] Smiley, *supra* note 517.

Ms. Herzberg's family settled with Uber out of court.[525] Uber, which had suspended testing of its self-driving vehicles during the pendency of the investigation, re-launched its self-driving cars nine months after the accident with significant new restrictions and safeguards.[526] One of the safety updates was the removal of the one-second braking delay.[527]

The operator during the crash, Rafaela Vasquez, was alone in the car and survived without injuries.[528] She was accused of watching television at the time of the accident.[529] Ms. Vasquez's attorneys contended in hearings that Vasquez was only listening to *The Voice,* which is equivalent to listening to the radio—which operators were allowed to do—and argued that the investigators mixed up which phone Vasquez was looking at in the seconds before the accident.[530] According to the defense, at the time of the accident, Ms. Vacquez was checking her phone for company Slack messages, as she was asked to do by Uber.[531] The defense court filings also indicate that several former Uber employees and whistleblowers were going to testify about safety lapses and risks ignored by Uber.[532]

A year after the crash, Arizona prosecutors cleared Uber of criminal liability. [533] In practical terms, this means that courts were never given the opportunity to consider Uber's contribution to the death of Herzberg.[534] However, Ms. Vasquez was charged with a felony—negligent homicide—and faced four to eight years in state prison.[535] In Arizona, the negligent homicide statute provides: "[a] person commits negligent homicide if with criminal negligence the person causes the death of another person…."[536] Ms. Vasquez pled guilty to one count of endangerment and was sentenced to three years of supervised probation, with no time in prison.[537] In Arizona, endangerment is defined as "recklessly endangering another person with a substantial risk of imminent death or physical injury."

The National Transportation Safety Board (NTSB) launched an investigation. According to the NTSB, the accident was caused by the programming lacking "the capability to classify an object as a pedestrian unless that object was near a crosswalk."[538] Because the car's programming did not allow it to recognize Herzberg as a pedestrian or a person—instead alternating between classifications of "vehicle, bicycle, and other"—it could not correctly predict her path and concluded that it needed to brake just 1.2 seconds before it struck her.[539] The report found that all aspects of the self-driving system were operating normally at the time of the crash, and that there were no faults or diagnostic messages.[540] As to why the software did not engage the emergency

---

[525] McCausland, *supra* note 518.
[526] THOMSON REUTERS, *supra* note 522.
[527] *Id.*
[528] National Transportation Safety Board Highway Accident Report HAR-19/03, November 25, 2019.
[529] Smiley, *supra* note 517.
[530] *Id.*
[531] *Id.*
[532] Smiley, *supra* note 518.
[533] *Id.*
[534] *Id.*
[535] *Id.*
[536] A.R.S. § 13-1102.
[537] A.R.S. § 13-1201.
[538] Smiley, *supra* note 517; National Transportation Safety Board Highway Accident Report HAR-19/03, November 25, 2019.
[539] *Id.*
[540] Johana Bhuiyan *Uber's Semi-Autonomous Car Detected The Pedestrian Six Seconds Before The Fatal Crash, A Federal Agency Says* VOX (May 24, 2018), www.vox.com/2018/5/24/17389120/uber-fatal-crash-arizona-semi-autonomous-ntsb-report.

brakes on its own, the NTSB noted that this passive approach was an intentional part of the design.[541] The Uber vehicle, a modified 2017 Volvo XC90, comes "factory equipped" with automatic emergency braking—but Uber's system disables this function.[542] Uber told the NTSB that emergency braking maneuvers are not enabled while the vehicle is under computer control, to reduce the potential for "erratic vehicle behavior."[543]

The NTSB's findings against Uber also included several criticisms of Uber.[544] The NTSB found that Uber kept an "inadequate safety culture," failed to protect operators from the phenomenon of "automation complacency"—humans' tendency to direct less attention to automatic processes that demand little input.[545] In fact, in the months before the crash, Uber had removed a requirement for there to be two operators in each car, which kept them more alert and adherent to the company's no-cell-phone policy.[546] Instead, solo operators were often looping the same monotonous route on hours-long shifts, left to self-police their usage of cell phones.[547] Uber also forbade operators from using handsets while driving, preferring that operators keep their phones handy in the car in order to get company Slack messages.[548]

Uber's own internal investigation into the crash concluded that the system detected Herzberg but did not react in time.[549] It also identified another factor: the company had tuned its system to not abruptly brake for "false positives" or objects that the vehicle was able to drive through.[550]

In the accident's aftermath, Uber told the NTSB that it "has since modified its programming to include jaywalkers among its recognized objects."[551] Additionally, Uber re-enabled the emergency braking system as part of the software update.[552] Uber also committed to adopting formal safety policies and procedures and brought in former NTSB Chair Christopher Hart to advise on and implement a new safety culture.[553]

2. Tesla death - 2019

In a similar case in Southern California, a driver was criminally prosecuted for failing to take his Tesla out of autopilot mode in a 2019 crash that resulted in two deaths.[554] The driver, Kevin Riad, had his hand on the wheel, according to the testimony of a Tesla representative, as his Tesla hit another car at 74 miles per hour.[555]

---

[541] Colin Dwyer, *NTSB: Uber Self-Driving Car Had Disabled Emergency Brake System Before Fatal Crash,* NPR (May 24, 2018), www.npr.org/sections/thetwo-way/2018/05/24/614200117/ntsb-uber-self-driving-car-had-disabled-emergency-brake-system-before-fatal-cras.
[542] *Id.*
[543] *Id.*
[544] Smiley, *supra* note 517.; National Transportation Safety Board Highway Accident Report HAR-19/03, November 25, 2019.
[545] *Id.*
[546] *Id.*
[547] *Id.*
[548] *Id.*
[549] Bhuiyan, *supra* note 540.
[550] *Id*.
[551] McCausland, *supra* note 518.
[552] CBC, *supra* note 521.
[553] Bhuiyan, *supra* note 540.
[554] Smiley, *supra* note 517.
[555] *Id.*

Mr. Riad was charged with manslaughter and gross negligence.[556] Prosecutors said the Tesla's Autosteer and Traffic Aware Cruise Control were active at the time of the accident.[557] There was no direct evidence at trial that Riad's car ran a red light, but witnesses testified that the light was, in fact, red.[558] Riad's defense attorney called no witnesses, arguing instead that Riad's actions—driving 74 mph on a surface street—did not rise to "gross negligence" and should not be considered a felony.[559] He ultimately pleaded no contest to two felony counts of vehicular manslaughter and was sentenced to two years of probation, avoiding prison.[560]

The families of both victims have filed separate lawsuits naming Riad and Tesla Motors Inc. as defendants in Los Angeles County Superior Court.[561] According to one of the complaints, Riad had been cited at least six times for moving violations in the three years before the crash, and the car was traveling at an "excessively high rate of speed" when it crashed.[562]

Thus, at least through early 2022, technology users faced a disproportionate share of legal responsibility or negative outcomes compared to the technology providers or developers. However, the tide has begun to turn.

3. Tesla Victory – 2020

Justine Hsu, a Los Angeles resident, sued Tesla in 2020, alleging her Tesla Model S swerved into a curb while it was on Autopilot in 2019, causing the airbag to deploy "so violently it fractured Plaintiff's jaw, knocked out teeth, and caused nerve damage to her face."[563] She alleged that her Tesla had design defects—specifically, defects in the design of Autopilot and the airbag.[564] She requested that the jury award her more than $3 million in damages.[565]

Notably, the director of Autopilot software at Tesla testified that a 2016 video used by Tesla to promote its self-driving technology was actually staged, to show capabilities, such as stopping at a red light and accelerating at a green light, that the system did not have.[566]

Tesla denied liability for the accident. It said in a court filing that Hsu used Autopilot on city streets, despite Tesla's user manual warning against doing so.[567]

Following a trial in Los Angeles Superior Court, the jury awarded Hsu zero damages, finding that the airbag did not fail to perform safely, and that Tesla did not intentionally fail to disclose facts to her.[568] Hsu broke down in tears outside the courtroom after the jury delivered its verdict.[569]

---

[556] Hillel Aron *Judge Orders Trial in Tesla Autopilot Manslaughter Case,* COURTHOUSE NEWS SERVICE (May 19, 2022), www.courthousenews.com/judge-orders-trial-in-tesla-autopilot-manslaughter-case/.
[557] Tony Cabrera, *Driver of Tesla On Autopilot Must Stand Trial For Crash That Killed 2 In Gardena, Judge Rules,* ABC NEWS (May 20, 2022), abc7.com/post/tesla-gardena-crash-driver/11873142/.
[558] Aron, *supra* note 556.
[559] *Id.*
[560] *Id.*
[561] *Id.*
[562] *Id.*
[563] *California Jury Finds Tesla Autopilot Did Not Fail In Crash Case,* REUTERS (April 21, 2023) www.nbcnews.com/business/business-news/california-jury-finds-tesla-autopilot-not-fail-crash-case-rcna80902.
[564] *Id.*
[565] *Id.*
[566] *Id*.
[567] *Id*.
[568] *Id*.
[569] *Id*.

Interviews with jurors revealed that, while the jurors felt badly for Hsu, they ultimately determined that Autopilot was not at fault.[570] The jurors gave credence to Tesla's theory of the case—that Hsu was distracted, and that the car comes with clear warnings that a driver needs to always be cognizant of what is happening in the car and be ready to react.[571] The jury also cited the audible and visual warnings for the driver, indicating that it is the driver's responsibility to maintain awareness.[572] Hsu's attorney stated that, while he understands the jury believed his client was distracted, she only received a warning to put her hands on the wheel less than a second before the curb strike, which was not an adequate time for her to react and avoid the curb collision.[573]

This was the first case to go to verdict involving a partially automated driving software.[574] The jury handed Tesla a sweeping win, finding that the car maker's Autopilot feature did not fail to perform safely.[575] Tesla is also under investigation by the U.S. Department of Justice and the National Highway Traffic Safety Administration over its claims about self-driving capabilities and the safety of the technology, respectively.[576]

4. Settlements

As Tesla was preparing for the *Hsu* trial, it settled cases with other victims, and was able to avoid jury trials and potentially adverse verdicts. Once such case, which was settled less than a week before jury selection was to begin, involved the highly publicized death of Apple engineer Walter Huang. Walter Huang was killed when his Tesla struck a concrete highway median in Silicon Valley on March 23, 2018.[577] The National Transportation Safety Board, in its investigation, found that Autopilot was engaged for nearly 19 minutes before the fatal crash, when the car, traveling at 71 mph, veered off the highway.[578]

Tesla said it believes Huang was responsible for the crash because investigators found he was playing a video game on his phone while Autopilot was engaged.[579] Huang did not brake or attempt to steer his car away from the concrete barrier before it crashed.[580] Although Huang's family acknowledges he was distracted while the car was driving, they argued Tesla is at fault because it falsely marketed Autopilot as self-driving software.[581] They alleged Tesla knew that Autopilot was not ready for public release and had flaws that made it unsafe.[582]

In addition to these settlements, in September and October 2023, U.S. District Judge Haywood Gilliam Jr. ruled that four of five plaintiffs in class-action lawsuits against Tesla were obligated to pursue their claims in individual arbitration due to signed arbitration clauses in their

---

[570] Abhirup Roy, Dan Levine and Hyunjoo Jin*, Exclusive: Tesla's Autopilot Never Claimed To Be Self-Pilot, Juror Says,* RUETERS (April 22, 2023), www.reuters.com/business/autos-transportation/teslas-autopilot-never-claimed-be-self-pilot-juror-2023-04-21/.
[571] *Id.*
[572] *Id*.
[573] *Id.*
[574] Reuters, *supra* note 563.
[575] *Id.*
[576] *Id.*
[577] David Goldman, *CNN Tesla Settles With Apple Engineer's Family Who Said Autopilot Caused His Fatal Crash*, CNN (April 8, 2024), www.cnn.com/2024/04/08/tech/tesla-trial-wrongful-death-walter-huang.
[578] *Id.*
[579] *Id.*
[580] *Id.*
[581] *Id.*
[582] *Id.*

purchase agreements.[583] The plaintiffs, who sued the company over allegedly deceptive "self-driving" and "Autopilot" claims, had unsuccessfully argued the arbitration agreement was unconscionable and not clearly displayed during the online purchase process.[584] However, the court held that the electronic payment screens provided conspicuous notice of the order agreements and that a 30-day opt-out provision within the agreement was enforceable.[585]

5. Cruise Robotaxi Incident (2023)

A Cruise autonomous vehicle struck and dragged a pedestrian approximately 20 feet after she was initially hit by a human-driven car.[586] The robotaxi stopped briefly but then attempted a "pull-over maneuver," failing to detect the pedestrian trapped underneath.[587] This resulted in severe injuries and an eventual settlement exceeding $8 million, and perhaps as much as $12 million.[588] Investigations revealed that the vehicle misclassified the collision as a side impact, lost track of the pedestrian, and incorrectly believed it needed to reposition, despite already being near the curb.[589]

The incident exposed critical limitations in AI perception and decision-making, including loss of object tracking (the system "forgot" the pedestrian after the initial collision); sensor blind spots (Lidar and camera systems did not fully detect the pedestrian's body under the vehicle); and faulty logic (the algorithm prioritized pulling over rather than executing an emergency stop).[590] This case showed notable gaps in Cruise's safety-critical programming.[591] Experts argue that conservative operational policies—such as requiring remote operator confirmation or maintaining an in-vehicle safety driver—could have prevented the dragging event.[592]

Cruise faced multiple investigations by the California Department of Motor Vehicles, National Highway Traffic Safety Administration, the Department of Justice, and the Securities and Exchange Commission.[593] The company agreed to pay a $500,000 criminal fine for making a false report to federal regulators about the incident.[594] Additionally, the California Public Utilities

---

[583] Jon Brodkin, *Judge Upholds Tesla Arbitration Agreement That Drivers Called "Unconscionable,"* ARS TECHNICA (October 2, 2023), arstechnica.com/tech-policy/2023/10/judge-upholds-tesla-arbitration-agreement-that-drivers-called-unconscionable/.
[584] *Id.*
[585] *Id.*
[586] Abhirup Roy, *How GM's Cruise Robotaxi Tech Failures Led It To Drag Pedestrian 20 Feet*, REUTERS (January 26, 2024), www.reuters.com/business/autos-transportation/how-gms-cruise-robotaxi-tech-failures-led-it-drag-pedestrian-20-feet-2024-01-26/.
[587] *Id.*
[588] Troy Wolverton, *Cruise Paying up to $12M to Woman Hit By Its Car In SF*, SAN FRANCISCO EXAMINER (May 15, 2024), www.sfexaminer.com/news/technology/cruise-reaches-settlement-with-woman-dragged-by-its-car/article_5946c74e-1314-11ef-af45-db35d72ccefe.html.
[589] *Id.*
[590] Philip Koopman, *Lessons from the Cruise Robotaxi Pedestrian Dragging Mishap*, CORNELL UNIVERSITY arXIV (JUNE 7, 2024), arxiv.org/abs/2406.05281.
[591] *Id.*
[592] *Id.*
[593] David Shepardson, *GM's Cruise Self-Driving Unit To Pay $1.5 Million Fine Over Crash Disclosure*, REUTERS (September 30, 2024), www.reuters.com/business/autos-transportation/gm-self-driving-unit-cruise-pay-15-million-fine-over-crash-disclosure-2024-09-30/.
[594] United States Attorney's Office, Northern District of California Press Release, *Cruise Admits To Submitting A False Report To Influence A Federal Investigation And Agrees To Pay $500,000* (November 14, 2024), www.justice.gov/usao-ndca/pr/cruise-admits-submitting-false-report-influence-federal-investigation-and-agrees-

Commission fined Cruise $112,500 for withholding information from state regulators under a deferred prosecution agreement.[595] Its driverless permits were suspended, and operations halted nationwide.[596] GM also indefinitely suspended plans to use its self-driving Origin vehicle that does not have a steering wheel.[597] GM later cut Cruise's budget by $1 billion and replaced most of its leadership team.[598]

6. The tide turns – Tesla liability (2025)

On August 5, 2025, a federal jury in Miami found Tesla partially liable in a fatal crash involving its Autopilot system, ordering the company to pay $329 million in a wrongful death and personal injury lawsuit.[599] The verdict arises from a 2019 collision in Key Largo, Florida, which resulted in one death and left another person with serious injuries.[600] Jurors awarded plaintiffs $129 million in compensatory damages and $200 million in punitive damages.[601] This is the first time Tesla has been found liable at trial for a third-party death linked to its driver-assistance technology.[602]

The collision occurred on April 25, 2019, when George McGee drove a Tesla Model S through a stop sign and traffic light before crashing into a parked Chevrolet Tahoe.[603] The victims were standing beside the SUV when it was struck.[604] Benavides Leon, who was just 22 years old, was thrown 75 feet and pronounced dead at the scene.[605] Her boyfriend, Angulo, sustained severe injuries including a traumatic brain injury and broken bones.[606]

McGee had activated Autopilot prior to the crash but became distracted while reaching for his dropped phone.[607] At trial, plaintiffs argued that Tesla's system failed to alert McGee or intervene as the vehicle entered the intersection.[608]

Plaintiffs also claimed that Tesla promoted the technology as more capable than it was in practice and failed to limit its use to appropriate road conditions.[609] At trial, evidence showed that

---

pay#:~:text=The%20criminal%20information%20alleges%20that,the%20secondary%20movement%20and%20dragging.

[595] Shepardson, *supra* note 593.

[596] CBS NEWS, *GM to Stop Funding Troubled Cruise Autonomous Vehicle Unit, Abandoning Robotaxis* (December 10, 2024), www.cbsnews.com/sanfrancisco/news/gm-stop-funding-troubled-cruise-autonomous-vehicles-robotaxis-san-francisco/.

[597] Shepardson, *supra* note 593.

[598] Graham Hope, *GM to Cut Cruise Self-Driving Car Spending by $1 Billion,* IOT WORLD TODAY (January 31, 2024), www.iotworldtoday.com/transportation-logistics/gm-to-cut-cruise-self-driving-car-spending-by-1-billion.

[599] Alexandra Agraz, *Jury Awards $329 Million in Tesla Autopilot Wrongful Death Case,* LAW COMMENTARY (August 05, 2025), www.lawcommentary.com/articles/jury-awards-329-million-in-tesla-autopilot-wrongful-death-case.

[600] *Id.*

[601] *Id*

[602] *Id.*

[603] *Id*.

[604] *Id.*

[605] *Id.*

[606] Singleton Schreiber, LLP press release (August 1, 2025), www.singletonschreiber.com/newsroom/pressreleases/singleton-schreiber-llp-wins-243-million-jury-verdict-for-victims-of-fatal-tesla-autopilot-crash#:~:text=Miami%2C%20FL%20%E2%80%94%20Singleton%20Schreiber%20founding,were%20sitting%20near%20the%20roadway.

[607] Agraz, *supra,* note 599.

[608] *Id.*

[609] *Id.*

Tesla designed Autopilot for use on controlled-access highways but did not restrict its use to such roads.[610] Despite these known limitations, the company allowed drivers to activate the system in local residential areas and marketed it with statements suggesting the technology performed better than a human driver.[611] "Tesla designed Autopilot only for controlled access highways yet deliberately chose not to restrict drivers from using it elsewhere, alongside Elon Musk telling the world Autopilot drove better than humans," said Brett Schreiber, lead trial counsel for the plaintiffs.[612]

Tesla's legal team contended the crash resulted from driver error and stated that McGee had pressed the accelerator, overriding Autopilot.[613] The company maintained that the system requires drivers to remain fully attentive and prepared to take control at all times.[614]

The plaintiffs cited Tesla's promotional materials, including a 2016 video that appeared to show a vehicle driving without human input.[615] In prior testimony unrelated to this case, a senior Tesla engineer acknowledged that the video was staged and did not accurately reflect the software's functionality.[616] Attorneys for the victims argued that such marketing was misleading and created confusion about the system's true capabilities, encouraging misuse.[617]

Jurors ultimately placed 67% of the fault in their contributory negligence finding on McGee, who admitted he took his eyes off the road after dropping his phone, and 33% of the blame on Tesla.[618] The jury awarded $59 million to Benavides' parents, $70 million to Angulo, and $200 million in punitive damages.[619] The compensatory damages were reduced to about $42.5 million to reflect Tesla's share of fault.[620] The rest of the blame was assigned to the driver, who had already settled with the victims and their families before the Tesla trial began.[621]

Tesla, which is headquartered in Texas, has indicated that it plans to appeal, calling the punitive damages unconstitutional and arguing Florida law sets a high bar for such awards.[622] The company continues to claim the crash was caused solely by driver distraction and that Autopilot was not the true culprit.[623] The company had previously refused a settlement demand from plaintiffs of $60 million, which in retrospect was a painful miscalculation, given the $242 million verdict.[624]

This is the first third-party wrongful death case involving Tesla's Autopilot to reach a jury verdict. Unlike the previous California case, which cleared Tesla of liability when the plaintiff was the driver of the Tesla vehicle, this case involved innocent pedestrians.[625] This victory for

---

[610] Singleton Schreiber, LLP, *supra* note 606.
[611] *Id.*
[612] *Id.*
[613] Agraz, *supra,* note 599.
[614] *Id.*
[615] *Id.*
[616] *Id.*
[617] *Id.*
[618] William F. Anzalone, *Jury Finds Tesla Autopilot Defective in Landmark $329 Million Verdict – What It Means for Future Cases,* ANZALONE & DOYLE (October 7, 2025), www.anzalonelaw.com/jury-finds-tesla-autopilot-defective-in-landmark-329-million-verdict-what-it-means-for-future-cases/.
[619] *Id.*
[620] *Id.*
[621] Fred Lambert, *Tesla Settles Another Fatal Autopilot Crash Before It Gets To Trial*, ELECTIK (September 16, 2025), electrek.co/2025/09/16/tesla-settles-another-fatal-autopilot-crash-before-it-gets-to-trial/.
[622] Anzalone, *supra* note 618.
[623] *Id.*
[624] Lambert, *supra* note 621.
[625] *Id.*

plaintiffs has opened the flood gates, and there are currently dozens of new cases pending, many filed by the same firm that represented the Leon family and Angulo in their victory.[626]

7. Settlements Continue

On the heels of this disastrous loss, Tesla settled another pending lawsuit for an undisclosed amount, avoiding a jury trial that could have resulted in another adverse verdict which had the potential to be even worse given the publicity surrounding their recent loss in the Leon/ Angulo case. In the newly settled case, a 15-year-old boy was killed after a Tesla Model 3 slammed into his father's truck.[627]

The lawsuit alleged that Benjamin Maldonado was traveling with his teen son, Jovani.[628] The two were on their way home from a soccer tournament in their Ford Explorer on Interstate I-880 in Alameda County.[629] Traffic was starting to slow, and Maldonado activated his blinker before moving right. Seconds later, his car was rear-ended by a Tesla Model 3 with Autopilot engaged, causing the victim's vehicle to roll over and crash into the center barrier. Jovani was ejected from the passenger seat and killed.

The driver of the Tesla, who was also named as a defendant, was alleged to have been "passively sitting" in the vehicle with Autopilot mode on, traveling 70 miles per hour, without having his hands on the steering wheel for at least 14 seconds prior to the collision.[630]

The lawsuit accused Tesla of negligence, alleging that its Autopilot technology had design defects.[631] The family claimed defects in the Tesla's driver-assistance software caused the car to fail to react to conditions on the roadway.[632] They also accused the company of misrepresenting the self-driving capabilities of its cars and failing to install key safeguards to warn drivers to remain focused on the road.[633]

Tesla argued in court filings that its technology functioned as designed, that the driver was solely at fault, and that there was no evidence that the Model 3 driver's decision to take his hands off the wheel was influenced by public statements made by Chief Executive Officer Elon Musk that Teslas can drive themselves.[634]

However, an apparently gun-shy Tesla also settled a case arising from the December 2019 death of two people who were traveling through an intersection in Gardena, California, in a Honda Civic when a Tesla Model S, equipped with Autopilot, failed to stop at a red light and crashed into

---

[626] *Id.*
[627] Natalie Musumeci, *Tesla Dodges Trial And Settles Lawsuit Over A Deadly Autopilot Crash,* BUSINESS INSIDER (September 17, 2025), www.businessinsider.com/tesla-settles-lawsuit-over-deadly-autopilot-crash-california-2025-9#:~:text=Tesla%20has%20settled%20a%20lawsuit,to%20a%20request%20for%20comment.
[628] *Id.*
[629] Madlin Mekelburg, *Tesla Settles Another Fatal Crash Suit Ahead Of Jury Trial*, BLOOMBERG NEWS (September 17, 2025), www.columbian.com/news/2025/sep/17/tesla-settles-another-fatal-crash-suit-ahead-of-jury-trial/#:~:text=Model%20X,plaintiffs%20or%20dismissed%20by%20judges.
[630] Musumeci, *supra* note 627.
[631] *Id*.
[632] Mekelburg, *supra* note 629.
[633] *Id*.
[634] *Id.*

the victims' vehicle at high speed.[635] The settlement in this case is only with Tesla; trial is set to continue against the driver of the Model S vehicle and other defendants.

Also in 2025, Tesla lost a jury trial in the *Banner* case. A lawsuit was filed by the estate of Jeremy Banner, who died in a 2019 Autopilot crash. Just before dawn on March 1, 2019, the software engineer was heading to work on a semi-rural Florida highway in his 2018 Tesla Model 3, which he had purchased months earlier. While traveling almost 70 mph, Banner activated Autopilot and took his hands off the wheel. To his right, a tractor-trailer leaving a farm moved into his path. The Tesla did not detect it and neither it nor Banner braked or swerved. Ten seconds after Autopilot was activated, the car drove underneath the trailer, shearing off the roof and killing Banner instantly.

The estate filed suit and sought punitive damages, alleging that Tesla had specific knowledge of the Autopilot's defects through government investigations, warnings, and prior accidents, and yet continued to market the technology as safe.

The judge focused on the company's marketing and Musk's comments about Autopilot, and noted other deaths that have occurred during its use. The company says in court documents that it warns drivers that its cars are not fully self-driving, that they still must pay attention to the road and that they are ultimately responsible for steering and braking.

But the judge agreed that Banner's attorneys had provided enough evidence for the case to proceed. Banner's attorneys have argued that by naming the system Autopilot, Musk and Tesla implied that the cars are self-driving and do not require the driver's full attention. They also cite numerous comments Musk made years before Jeremy Banner's crash saying that Autopilot was already better than human drivers and would soon be autonomous. In support of their claim for punitive damages, plaintiff's counsel argued Tesla's conduct was not just negligent, but involved intentional and reckless decisions that led to the death of customers, including Jeremy Banner.

The attorneys also pointed to a 2016 marketing video for Autopilot that is still on the company's website. It begins with a statement reading, "The person in the driver's seat is only there for legal reasons. He is not doing anything. The car is driving itself." The Tesla then maneuvers through a town on winding roads in traffic. It halts at traffic lights and stop signs, avoids other cars, pedestrians and bicyclists and speeds up and slows down as appropriate. It then parallel parks itself. The camera is positioned to show that the man in the driver's seat never touches the steering wheel or pedals. Under questioning by Banner's attorneys, Tesla employees revealed that the car in the ad was programmed with mapping software not available to the public and "still performed poorly and even ran into a fence while filming." The video required several takes and was heavily edited, the attorneys say.

The judge wrote that, after reviewing the evidence, he could not "imagine how some ordinary consumers would not have some belief that the Tesla vehicles were capable of driving themselves hands free."[636]

The National Transportation Safety Board, which investigated the crash, said the truck driver was primarily to blame for pulling into traffic, but also said Banner and Tesla were at fault.

---

[635] Abhirup Roy and Mike Scarcella *Tesla Settles Two Lawsuits On 2019 California Crashes Related To Autopilot Software,* RUETERS (September 16, 2025), www.reuters.com/business/autos-transportation/tesla-settles-two-lawsuits-2019-california-crashes-related-autopilot-software-2025-09-16/.

[636] Terry Spencer, *Lawsuit Blaming Tesla's Autopilot For South Florida Driver's Death Can Go To Trial, Judge Rules,* NBC MIAMI (November 23, 2023), www.nbcmiami.com/news/local/lawsuit-blaming-teslas-autopilot-for-south-florida-drivers-death-can-go-to-trial-judge-rules/3167078/.

"An attentive driver would have seen the truck in time to take evasive action," the NTSB said of Banner. The Board said Tesla's Autopilot should have safeguards that do not allow the system's use on highways that have cross-traffic. The car should also make certain drivers using Autopilot remain engaged with their hands on the wheel.

A jury found Tesla partially at fault, awarding over $240 million in damages, including $200 million in punitive damages, with a finding that Tesla's Autopilot was defective and misleadingly marketed. (The trucking company had already reached a confidential settlement with Kim Banner and was no longer part of the lawsuit at the time of trial).

Tesla appealed the verdict, arguing that it sets a dangerous precedent for the automotive industry and could jeopardize efforts to develop and implement safer autonomous driving technology. The company contended that the jury was improperly influenced by emotionally charged evidence and that the decision failed to adequately consider the complex technical and regulatory environment surrounding autonomous vehicle development. Tesla further asserted that such rulings may discourage innovation by imposing disproportionate liability on manufacturers, even when systems are designed to meet or exceed existing safety standards.

On February 26, 2025, the Florida Fourth District Court of Appeal unanimously reversed the trial court's decision reasoning that Florida imposes a high bar on punitive damages claims.[637] Specifically, the court highlighted several key points related to claims of punitive damages in product liability cases: the level of negligence required to plead punitive damages in Florida requires conduct equivalent to establishing criminal manslaughter; and the Florida Supreme Court has all but eliminated punitive damage awards in product liability cases.[638] The court emphasized that Tesla's Autopilot system met industry standards and that drivers are responsible for staying alert while using the technology. Additionally, Florida law presumes a product is not defective if it complies with applicable government regulations. The case was remanded for a new trial, however, petitioner accepted a settlement offer before the second trial. This case will likely not influence cases in other states seeking punitive damages since Florida's law is unusually restrictive with regard to the imposition of punitive damages.

The terms of all three agreements are confidential.

8. The Future

It is important to remember that the cases that are currently coming up on trial dockets around the country are crashes that occurred in 2018 and 2019. The newly filed cases, which were filed in the wake of the McGee case, are unlikely to be heard before 2030. In the meantime, Tesla has introduced its Full Self-Driving (FSD) feature, which it advertises can, with active driver supervision, handle tasks like navigating, changing lanes, and making turns. In addition, the pace of Tesla sales have increased since 2018. With the increased sales volume and new software, as more miles are driven, more accidents are bound to occur, and litigation will inevitably follow.

The fatal crash involving Uber's autonomous vehicle in Tempe, Arizona, exemplifies multiple systemic risks inherent in AI-driven transportation systems. Most critically, Risk 2 (threatening or intent to create harm) materialized when the vehicle's failure to correctly classify a pedestrian resulted in a loss of life, underscoring the catastrophic consequences of design flaws in safety-critical applications. The inability of the system to recognize jaywalking behavior and its delayed braking response reflect Risk 8 (inability to explain model outputs), as the decision-

[637] Tesla, Inc. v. Banner, No. 4D2023-3034 (Fla. Dist. App. Feb. 26, 2025).
[638] Banner, at 5.

making logic was opaque and misaligned with real-world scenarios, leaving investigators and operators unable to fully understand or anticipate system behavior. Furthermore, the reliance on limited object classification rules and calibration to avoid "false positives" implicates Risk 4 (algorithmic bias), as the system's performance was constrained by assumptions that did not generalize to diverse pedestrian behaviors. The disabling of factory-installed emergency braking and removal of dual-operator safeguards reveal Risk 7 (vulnerabilities in generative AI systems) and a deficient safety culture, which amplified automation complacency and increased operational risk. Finally, the incident triggered significant Risk 9 (compliance and reputational risk), as Uber faced regulatory scrutiny, litigation, and reputational damage, prompting major revisions to its safety protocols. Collectively, this case illustrates how technical limitations, inadequate governance, and human factors converge to create compound risks in autonomous systems, reinforcing the need for robust safety engineering, transparency, and accountability in AI deployment.

The 2019 Tesla autopilot crash in Southern California, which resulted in two fatalities and subsequent criminal prosecution of the driver, illustrates several critical risks associated with semi-autonomous vehicle technology. Most notably, Risk 2 (Threatening or intent to create harm) is implicated, as the failure of the autopilot system to prevent a high-speed collision led to loss of life. The incident also reflects Risk 8 (Inability to explain model outputs), given the opacity surrounding how Tesla's Autosteer and Traffic-Aware Cruise Control systems interpreted traffic signals and managed braking decisions, leaving courts and investigators unable to fully assess system accountability. Furthermore, Risk 4 (Algorithmic bias and misrepresentation) may be relevant if the system's design assumptions—such as reliance on ideal driving conditions and a limited subset of roads—did not generalize to complex urban environments, increasing the likelihood of error. The case also raises Risk 9 (Compliance and reputational risk), as Tesla faced civil litigation and heightened scrutiny over marketing claims that may have overstated the safety and reliability of its autopilot features. Finally, the disproportionate legal burden placed on the human operator, despite systemic design limitations, underscores governance gaps in liability frameworks for AI-assisted driving. Collectively, this case demonstrates how technical limitations, inadequate transparency, and unclear accountability mechanisms converge to create compound risks in the deployment of autonomous systems.

The Cruise robotaxi accident, in which an autonomous vehicle struck and dragged a pedestrian, also exemplifies multiple high-severity risks associated with AI-driven mobility systems. Most critically, Risk 2 (threatening or intent to create harm) materialized when the system's failure to execute an emergency stop resulted in severe injuries. The misclassification of the collision as a side impact, combined with the algorithm's decision to prioritize a pull-over maneuver rather than braking, underscores Risk 8 (inability to explain model outputs), as the logic behind these decisions was opaque and misaligned with safety-critical priorities. Additionally, the loss of object tracking and sensor blind spots implicate Risk 7 (vulnerabilities in generative AI systems), revealing technical weaknesses in perception and situational awareness. The flawed training and operational logic, including disabling safety measures and failing to anticipate jaywalkers, reflect Risk 4 (algorithmic bias and misrepresentation), as the system was optimized for routine conditions rather than rare but catastrophic scenarios. The regulatory fallout, including permit suspensions, multimillion-dollar settlements, and federal investigations, highlights Risk 9 (compliance and reputational risk), demonstrating how inadequate safety culture and misleading advertising can escalate legal and financial exposure. This case illustrates the convergence of

technical, ethical, and governance failures in autonomous systems, reinforcing the need for robust safety engineering, transparency, and regulatory compliance in AI deployment.

Finally, the landmark 2025 jury verdict against Tesla in a wrongful death case involving its Autopilot system underscores several critical risks associated with semi-autonomous driving technologies. Foremost, Risk 2 (threatening or intent to create harm) was realized when the system failed to prevent a fatal collision, despite being engaged at the time of the crash. The inability of Autopilot to alert the driver or intervene as the vehicle entered an intersection reflects Risk 8 (inability to explain model outputs), as the system's operational logic and limitations were opaque to users and investigators. Tesla's decision to allow Autopilot activation on local roads—despite designing it for controlled-access highways—introduces Risk 4 (algorithmic bias and misrepresentation), as the system was deployed in contexts for which it was not optimized, increasing the likelihood of error. Furthermore, Tesla's marketing practices, including promotional materials that overstated Autopilot's capabilities, implicate Risk 9 (compliance and reputational risk), given the resulting litigation, punitive damages, and regulatory scrutiny. These failures collectively highlight the convergence of technical limitations, governance gaps, and misleading representations, reinforcing the need for transparent design, operational safeguards, and truthful communication about AI system's capabilities in safety-critical domains.

An AUP could have reduced some risks in these cases, but would not have fully prevented harm. An AUP sets clear rules for how systems can be used, defines user responsibilities, and restricts unsafe practices—such as using Autopilot outside its intended domain, disabling emergency braking, or operating without proper supervision. In incidents like Uber's Tempe crash, Tesla's Autopilot failures, and Cruise's robotaxi accident, a strong AUP could have mandated safeguards like dual operators, geofencing, driver monitoring, and truthful marketing, reducing misuse and expectation gaps. However, an AUP alone cannot fix technical flaws like object misclassification, sensor blind spots, or opaque decision-making. To be effective, an AUP must be paired with engineering controls, transparency, and regulatory compliance. In short, an AUP is necessary for governance and accountability, but insufficient in the autonomous driving context without robust safety design and enforcement mechanisms.

VI. CONCLUSION AND RECOMMENDATIONS

This paper examines the critical importance of implementing Acceptable Use Policies (AUPs) for AI tools in organizational contexts. It is clear that, while generative AI enhances productivity, its integration without robust governance mechanisms amplifies organizational risk. Proactive risk identification requires companies to assess potential risks such as data privacy violations, algorithmic bias, intellectual property misuse, and security vulnerabilities before implementing AI solutions. Once an organization commits to adopt or incorporate AI, it must establish well-defined governance frameworks to ensure responsible, compliant, and secure implementation. Once AI is adopted or integrated into organizational processes, establishing a comprehensive AUP becomes essential.

The implementation of an AUP is no longer a peripheral consideration for organizations; it is a strategic necessity in today's technology-driven business environment. Given the significant potential liability, AUPs must be intentionally drafted, comprehensive in scope, regularly reviewed, and rigorously enforced. A well-structured AUP provides a clear framework for responsible technology use, thereby reducing operational, legal, and reputational risks while promoting compliance with regulatory standards. For companies, the benefits extend beyond risk

mitigation—AUPs foster a culture of accountability, enhance data security, and ensure employees understand their role in safeguarding organizational integrity.

As artificial intelligence becomes increasingly integrated into business processes, traditional AUPs must evolve to address new and complex challenges. AI introduces risks such as algorithmic bias, data privacy breaches, intellectual property concerns, and misuse of generative tools. These risks, if unmanaged, can lead to significant ethical and legal consequences. Therefore, organizations must adopt a proactive approach by developing AI-focused AUPs.

Of primary importance in an AUP is the establishment of clear boundaries for AI usage. Companies should define what constitutes acceptable and prohibited use of generative AI tools within the organization. This includes specifying tasks where AI may be leveraged (*e.g.,* drafting non-sensitive content) and explicitly prohibiting activities such as uploading proprietary code, confidential documents, or personally identifiable information. Transparency and accountability frameworks for AI decision-making, including documentation and audit trails, is critical to manage enterprise risk. Once these frameworks are in place, AI systems must be continuously monitored and regularly re-evaluated for performance, fairness, and security.

Companies should also zealously safeguard sensitive information through structured governance. The implementation of comprehensive governance structures that outline confidentiality requirements and data handling protocols is paramount. Employees should understand that generative AI platforms often retain user inputs for model training, creating persistent exposure risks for the organization. Policies must emphasize that sensitive data—including intellectual property, financial records, and customer information—cannot be shared with external AI systems under any circumstances.

It is also important that companies promote responsible and transparent AI adoption. Employee training should demonstrate the ethical and legal implications of AI use. Companies should also incorporate guidelines for bias mitigation, accuracy verification, and transparency in outputs. Human oversight should be required for critical decisions and disclosure should be mandated when AI-generated content is used in official communications.

Organizations should avoid over-promising AI capabilities or misrepresenting AI-generated outputs as human-authored work. In high-stakes contexts, such as legal, medical, financial, or academic publications, verification and validation processes must be mandatory prior to release or publication to ensure accuracy, integrity, and regulatory compliance. Corporate AUPs should also address the nine risks identified by Gartner, notably including intellectual property leakage, algorithmic bias, and regulatory noncompliance. The policies should require bias audits for AI tools, verification of outputs, and regular compliance checks aligned with industry standards and applicable laws and regulations. Organizations should also prepare for worst-case scenarios, such as model failures or adversarial attacks, by having clear response protocols and fallback systems.

It is crucial to strengthen organizational resilience against emerging AI threats, including malicious third parties. Robust monitoring and rigorous enforcement mechanisms to ensure compliance and detect misuse early, including real-time monitoring, reporting, and disciplinary procedures for policy violations are required. The establishment of escalation protocols for incidents involving data breaches or misuse of AI systems is also essential. Again, regular and comprehensive employee training on evolving AI risks and best practices is imperative.

Finally, risk-aware practices should be embedded into corporate AI strategies. Organizations must treat risk management as a core component of their AI adoption, rather than as an afterthought. This involves integrating risk considerations into every stage of the AI lifecycle,

from design and development to deployment and monitoring. Risk-aware practices are not just technical, and are not just pages in an employee manual; they require cultural adoption and organizational integration. Embedding risk-aware practices ensures compliance with frameworks like the GDPR, emerging AI regulations, and industry-specific guidelines and regulations.

Ultimately, well-defined governance frameworks, comprehensive AUPs, and robust employee training are indispensable for balancing innovation with risk management in the era of generative AI. By adopting these measures, organizations can not only mitigate AI-related risks, but can also position themselves as credible and forward-thinking organizations amid rapid technological advancement. A dynamic, forward-thinking AUP serves as a cornerstone of ethical governance and financial stewardship, enabling sustainable growth and reinforcing stakeholder confidence in an increasingly AI-driven business landscape.

The SOUTHERN ACADEMY OF LEGAL STUDIES IN BUSINESS wishes to express its sincere appreciation to:

SOUTH-WESTERN
CENGAGE Learning

For Helping Sponsor the 2026
SALSB Conference

The Southern Law Journal is an official publication of the
Southern Academy of Legal Studies in Business

Listed in Ulrich's International Periodical Directory and in Cabell's Directory

Available at www.southernlawjournal.com and through
EBSCO, an electronic university database