2024 Design, Automation & Test in Europe Conference (DATE 2024)
Special Initiative "Autonomous Systems Design"

Corporate Governance and Management of AI-Driven Product Development: Vehicle Automation

William H. Widen
School of Law
University of Miami
Miami FL USA
w.widen@miami.edu

Marilyn C. Wolf
School of Computing
University of Nebraska -- Lincoln
Lincoln NE USA
https://orcid.org/0000-0002-4742-0841

***Abstract*— This essay explores the interplay between proper corporate governance and engineering expertise in developing products that use artificial intelligence (with a focus on vehicle automation) and considers how an organization might balance maximizing earnings with the public interest in safe and secure AI-driven products. The essay recommends that for oversight directors use a management model with structures of communication and reporting which provides for more direct engagement with engineers and product managers.**

Keywords—automated vehicle, certification, corporate governance, cyber-physical system, engineering ethics, machine learning, safety, security, self-driving car, self-driving technology

I. Introduction

This essay is a preliminary exploration of the interplay between proper corporate governance and engineering expertise in developing products that use artificial intelligence (AI), with a focus on vehicle automation. The goal is to understand better how an organization might balance maximizing earnings with the public interest in safe and secure AI-driven products and the challenges an organization might face in achieving that balance under principles of U.S. corporate law. The essay recommends that directors should, as part of oversight, use a management model with structures of communication and reporting that provides for more direct engagement with engineers and product managers. Corporations organized outside the U.S. might use U.S. principles of proper board oversight, including terms in settlement orders and consent decrees in cases of failed oversight, to enhance safety and security of AI-driven products regardless of any potential director liability for oversight lapses under local company law.

Recent events at Tesla [1], Cruise [2] and Open AI, [3] show how a corporation may experience a conflict between profit seeking and protecting the public from harms caused by, or related to, the design, testing and deployment of its products—with adverse consequences for an organization that prioritizes profit while ignoring safety [4]. Corporate law seeks to find a proper balance by requiring that a board of directors provide top-down oversight of an organization's activities [5, 6], including ensuring that managers have established appropriate risk management systems [7]. Case law suggests that boards should pay particular attention to risks posed by technology (such as cybersecurity risk management), and risks that affect mission critical aspects of an organization's business. A heightened oversight duty applies to ensure compliance with laws—particularly in heavily regulated lines of business.

The U.S. National Institute of Standards and Technology (NIST) highlights the importance of corporate governance to development of safe and secure AI-driven products in several initiatives. The public draft of Cybersecurity Framework 2.0 recognizes the importance of corporate governance by adding a GOVERN function [8]. This follows NIST's January 2023 advice in its Artificial Intelligence Risk Management Framework (AI RMF 1.0) which also includes a GOVERN function [9]. Techniques for managing conflicts between the pursuit of profit and the public interest in safety and security should interest industry participants and STEM students as a practical problem in engineering ethics which, in the vehicle automation field, tends to focus on impractical issues such as the "Trolley Problem" familiar from introductory ethics classes.

II. Recent Events & Issues

The U.S. National Highway Traffic Safety Administration (NHTSA) recalled Tesla vehicles which contain automated driving features. California suspended Cruise's permission to operate its uncrewed robotaxis after a serious pedestrian accident. Cruise's CEO resigned, followed by the departure of nine other executives. OpenAI's board replaced its CEO for a brief period, but multiple complaints resulted in the CEO's reinstatement, with certain members who supported the dismissal leaving the board instead. Each case reflects a possible failure of board oversight.

A significant management challenge arises when board members tasked with governing and overseeing AI-driven product development have failed to establish a safety culture or have insufficient expertise, information, or time to evaluate the technical merits and pitfalls associated with company technology—exacerbating risks created by the presence of a founding CEO or technology innovator such as at Tesla, Cruise and OpenAI.

Certain generally recognized problems for corporate governance cut across industry sectors: first, concentration of risk management oversight in an overburdened audit committee of the board; second, a disconnect between board members' perception of their own technical expertise and the expertise that board members actually possess; and third, a systemic failure of organizations to follow optional recommendations, standards and best practices from regulators, professional organizations and industry associations.

979-8-3503-4859-0/DATE24/© 2024 EDAA

III. How Corporations Operate

Fiduciary Duty to Pursue Profits: Any analysis of corporate governance challenges begins with a clear understanding of how corporations operate. One cannot give credence to public relations narratives such as those at Tesla, Cruise, and OpenAI which emphasize the promotion of public safety and security while ignoring the real purpose of the typical corporation—the pursuit of profit. To be sure, there is nothing wrong with pursuing profits. Officers and directors have a fiduciary duty to maximize profits for their shareholders but no duty to promote public welfare.

These three cases illustrate why society should not rely on internally generated motivations or novel corporate ownership structures to promote a corporation's pursuit of the public good (instead of profit maximization). Three external factors provide motivations for a corporation to act in the public interest. First, as a creature of law, a corporation has an obligation to comply with laws, regulations, and rules adopted to promote the public interest. A board has a duty to oversee that operations comply. Second, tort law makes corporations liable for harms proximately caused by their negligent actions and distribution of defective products. The threat of adverse money judgments provides organizations with a financial motive to avoid creating unreasonable risks. Third, regulators, professional organizations and industry associations often recommend following optional procedures, standards, and best practices. Following recommendations may provide marketing benefits to an organization and indirectly help with defending a lawsuit.

If a corporation has allegedly violated a law, a court may require by order, settlement, or consent decree that the organization implement detailed corporate governance steps such as at Boeing [10] and Cummins [11]. Engineers have a particularly important role in verifying compliance with court-imposed governance procedures related to technical requirements.

Governance vs. Management: A common description of corporate governance structure is that the board of directors "governs" the organization, while senior executive officers "manage" the organization. The chief executive officer coordinates interactions between the board and the other executives. Corporate governance includes *oversight* of management as part of the governance role.

To avoid liability in a corporate setting for breach of an oversight duty, directors must make a good faith effort to establish reasonable compliance and reporting systems to monitor compliance with laws, rules, and regulations. Oversight also includes putting in place systems for monitoring risks presented by technology, including cybersecurity risk management. Oversight establishes mechanisms and then monitors that they function as intended.

Following steps that a board takes to fulfill its oversight duties under U.S. corporate law supports development of safe and secure technology as a beneficial byproduct in any jurisdiction. Effective oversight begins by selecting a management model to implement compliance and reporting. Techniques to strengthen oversight appear in court settlements and consent decrees applicable to cases of failed oversight such as at Boeing for the 737 MAX or at Cummins for diesel engine emissions and could inform the nature of oversight mechanisms a company might adopt to promote safety and security without the compulsion of a court order.

IV. Selecting a Management Model & Governance Structures

A board of directors should use a hybrid management model to manage complex technology development—a combination of top-down and bottom-up control and reporting—because that model addresses the problem of insufficient board expertise and information. Board members can be educated about technology issues and risks by an ongoing, iterative exchange of information from persons with product specific technical knowledge—exchanges which may not occur in traditional top-down, command and control management models and their related forms of communication [12].

In Boeing derivative litigation over the 737 MAX crashes, the Delaware chancery court stated that "[s]tockholders have come to this Court claiming Boeing's directors and officers failed them in overseeing mission-critical airplane safety to protect enterprise and stockholder value" [13].

The court addressed the narrow question of whether the Boeing directors faced a substantial likelihood of liability for Boeing's losses and concluded that stockholders had successfully pled two potential sources of board liability: a complete failure to establish a reporting system for airplane safety; and, on "turning a blind eye to a red flag representing airplane safety problems."

No board committee had been assigned the specific task of overseeing airplane safety. Second, no committee description of responsibilities included mention of oversight for airplane safety. Third, the strong implication was that the audit committee had too much on its agenda to conduct proper oversight of aircraft safety because the audit committee was the primary supervisor of all risk and compliance matters for the company.

These shortcomings resemble oversight failures at Blue Bell Creameries USA, Inc. for a recall of products following a listeria outbreak in 2015 in which three persons died [14]. The plaintiffs had alleged that Blue Bell "had no [board] committee overseeing food safety, no full board-level process to address food safety issues, and no protocol by which the board was expected to be advised of food safety reports and developments."

The failure to implement a management model with appropriate lines of reporting and communication can create "responsibility gaps" in the development of vehicle automation, as discussed by Prof. Cummings [15]. She proposes that "engineers responsible for testing [become] the new first-line actors in AI systems" because "[m]ore needs to be done to hold company executives and testing lead engineers accountable." Her essay stresses the importance of selecting a model to understand the cause of accidents, using the "Swiss Cheese Accident Causation Model" as a starting point. She then proposes to supplement that model with a new "Taxonomy for AI Hazard Analysis", using three automated

vehicle accident cases to explain the benefits of the new taxonomy she proposes.

While a board will not manage the day-to-day details of ongoing testing of vehicle automation systems—that is a task beyond oversight—we can expect a board to instill a robust safety culture throughout an organization particularly when safety is mission critical to the business (as is the case for vehicle automation). We also might expect the board to require that senior management, in consultation with engineers and product managers, adopt a model to understand the proximate causes of automated vehicle accidents.

Effective oversight may require designation of a senior executive officer in charge of compliance with technical standards and management of risks associated with new AI-driven products who reports directly and often to the board or a board committee (ideally a safety committee not an audit committee). This position would differ from the role played by a traditional corporate compliance department which often focuses on matters other than safety and conformity of a product to a standard, instead monitoring such matters as compliance with the Foreign Corrupt Practices Act.

Tesla's Operations: Tesla's 2023 public filings with the U. S. Securities and Exchange Commission (SEC) suggest several shortcomings in its oversight structure which resemble failings in cases in which plaintiffs alleged a breach of the duty of oversight that survived a motion to dismiss. Tesla's board does not have a dedicated product safety committee which might focus on safety of self-driving technology. The audit committee performs general oversight of risk management in addition to oversight of finance and accounting matters. The audit committee's charter is twice the length of the charters of the board's other committees. The audit committee appears overburdened both because of the length of its charge and because the 2023 Proxy describes a broad risk management role:

> "In addition to overseeing key risks in the areas of data security and privacy, crisis risk management, ethics and compliance, and ESG, as discussed below, the Audit Committee is also responsible for overseeing risks in other areas of our business and operation."

Though the description specifically mentions data security and privacy, it makes no mention of product safety generally, or self-driving systems. The 10-K filed in 2023 compares Tesla's Autopilot and full self-driving (FSD) systems to "system[s] that airplane pilots use" yet Tesla's self-driving technology presents greater risk of operator error while interacting with these systems because its customers who act as "beta testers" for self-driving technology are not trained like pilots. The 2023 Proxy Statement mentions "safety" once and executive compensation does not appear to include metrics for achieving safety goals.

The 2023 Proxy Statement identifies some board members with experience in the areas of risk and compliance, but none appear by educational background to have specific expertise with neural networks and the challenges they pose for safety of self-driving technology. Perhaps Tesla does better behind the scenes, but company SEC filings do not emphasize management structures that promote automation safety—suggesting a possible failure of board oversight.

These apparent shortcomings resemble the oversight failures at Boeing which were specifically addressed in the settlement of derivative litigation. But oversight of vehicle automation technology has an added complexity. The engineering behind aircraft is well understood and there is a well-established regulatory framework which addresses aircraft safety. In contrast, the technology behind vehicle automation is not well understood and neither NHTSA nor legislators have established a comprehensive regulatory scheme for safety. NHTSA merely requires accident reporting so it might regulate via recall after the fact. This places an increased burden for ensuring safety and security of self-driving technology on the interactions between engineers and the corporate governance function. This might require that management establish specific internal guidelines for product safety, security, and testing, with ongoing monitoring that the development teams comply with those guidelines.

Cruise/GM: Because Cruise operates as a majority owned subsidiary of General Motors, GM's public filings do not provide the necessary details to deconstruct possible shortcomings in governance structure that led to the failure at Cruise. It is reasonable to conclude, however, that Cruise's operation, as a subsidiary, created an additional layer of reporting that hindered communications from Cruise to the GM board about product development risk. Though GM became more directly involved after the San Francisco accident, it appears that GM acted like a passive investor with respect to oversight until a crisis occurred. This hands-off approach is somewhat surprising given the numerous press reports of mishaps at Cruise and well publicized controversy over regulatory approval of uncrewed operations.

Perhaps one lesson for development of AI-driven products from Cruise is that significant investors should act as engaged stakeholders, taking a more active role in oversight consistent with their ownership interest. Indeed, some case law suggests that a parent company's board can breach a duty of oversight with respect to operations at its subsidiary [16].

OpenAI: The drama at OpenAI has not resulted in any disclosed harm. However, it does suggest that a hybrid corporate structure using a not-for-profit parent with a majority owned for-profit subsidiary is unlikely to work as advertised to promote the public interest. In the end, OpenAI appeared to function in pursuit of profits by reinstating its CEO just as any other organization—with the much-touted hybrid structure contributing little to guard the public interest. Guarding the public interest remains primarily a task for law. The AI community has called for regulation [17]—a move reminiscent of Odysseus lashing himself to the mast of his ship so he might listen to the Sirens.

V. Levels of Compliance and Risk Management

Factors external to the corporation provide operating limitations that constrain profit-seeking activities (i.e., they do not arise organically within the corporation). These guardrails vary in their strength and specificity.

Compliance with Laws: A corporation has an obligation to comply with laws. Those charged with oversight as part of governance have a fiduciary duty to put in place corporate

structures and lines of reporting for the express purpose of compliance.

When a law incorporates by reference a technical standard [18] that applies to a product driven by complex technology, the corporate governance function overlaps directly with the product development function because both must ensure that the technical standard is met as a matter of verification.

Corporate and engineering methods complement each other when focused on mandatory compliance with laws, regulations, and rules which incorporate technical standards by reference because completion of an engineering verification process should satisfy any legal requirements imposed by incorporation of the technical standard by reference. The board simply needs to establish procedures for management to follow and monitor to assure satisfactory implementation of the verification process.

Best Practices Without the Force of Law: When a regulator, professional organization or industry association makes recommendations or publishes standards or best practices without the force of law, a different corporate governance challenge arises: whether, and to what extent, should the corporation follow the recommendation?

The unfortunate truth is that voluntary compliance regimes do not work well. The SEC confirmed this unfortunate fact in its release adopting cybersecurity disclosure requirements effective September 5, 2023, noting "[o]verall, we remain persuaded that, as detailed in the Proposing Release: under-disclosure regarding cybersecurity persists despite the Commission's prior guidance …" [19]. A board may be unaware of a failure to follow voluntary compliance regimes because senior management may consider such a decision to be the product of a cost-benefit analysis which management views as a business decision for executives, and not appropriate for board level review. In the automotive field, the voluminous literature makes review and selection of a best practice or standard a time-consuming task—though several standards prominently apply to automated vehicles—such as SAE J3018 and UL 4600 which a board should know about, perhaps even requiring executives to justify non-compliance as part of oversight.

Failures to follow consensus industry standards for vehicle automation are common in U.S. industry by ignoring the SAE J3018 recommendation to use safety drivers and the recommendations of UL 4600 to assess the safety case for an autonomous vehicle. Failure to follow a consensus industry standard can have franchise threatening consequences as evidenced by Cruise's failure to use safety drivers for operation of its immature robotaxi technology.

For optional practices and standards, corporate governance obligations do not overlap neatly with product development processes. Indeed, senior corporate officers might direct that an AI-driven product meet mandatory minimum legal requirements (but nothing more). The engineering design team may have chosen to comply with consensus industry standards without a contrary direction. A board may not be sufficiently informed about the nature and extent of optional regulatory recommendations, industry standards and best practices to oversee the process used by management to save costs by non-compliance. An infamous cost-saving measure gone bad relates to Ford's decision to remove a protective bladder from the gas tank of the Pinto to meet a target set by senior management [20].

As part of the oversight function, a reporting structure should advise the board about management decisions to ignore optional industry standards and regulatory recommendations, including a description of possible consequences of that decision. A chief safety and testing officer should express a view on non-compliance. Engineering input from the product design team could assist this process by providing cost estimates (including additional development time) for consideration by the board. A board might not approve a decision to ignore a standard if members understood that accepted methods to manage risk of accidents includes compliance with industry standards [21].

Market Incentives: Market discipline incentivizes a company to comply with some voluntary standards, such as ISO 26262 (functional safety standard for electrical and electronic systems in road vehicles) which does not have the status of law. But as experience with SAE J3018 and ISO 4600 demonstrates, this is not always the case.

Liability Rules: Tort law creates a general guardrail to constrain profit-making activities within reasonable limits by imposing negligence and product liability. An organization must take special care when evaluating products to ensure that it does not misunderstand the application of legal rules to the new product, or the risks associated with cost-saving measures. This is particularly true in vehicle automation where some companies take the position that they only have product liability for design defects, while others recognize that the law might treat a vehicle automation system as a "computer driver" which owes a duty of care to other road users just as human drivers do [22]. Limiting liability for vehicle automation to design defects provides a practical liability shield because neural networks are "black boxes" complicating liability attribution whereas imposing a duty of care on a computer driver creates familiar liability attribution for auto accidents based on negligent driving behavior.

VI. Soft Standards & Definitions

Professional organizations sometimes promulgate "soft standards" such as IEEE 7000 consisting of ethical product design procedures. Another soft standard is ISO 26000 which addresses corporate social responsibility. Compliance with soft standards typically involves following procedures for decision making as opposed to insuring verification and validation of a cyber-physical system.

The IEEE 7000 standard differs from a typical technical standard because one does not *verify* the conformity of a cyber physical system to a technical standard as part of ethics compliance. Similarly, one does not *validate* that a cyber physical system is fit for a purpose by following a standard process for ethical design. Rather, one might confirm that a product design had a certain provenance—that the design process included consideration of the interests of a variety of stakeholders and not just the needs of the intended user of the product as contemplated by IEEE 7000. Similarly, ISO 26000 provides guidance rather than requirements so it cannot be

certified like other ISO standards (though a third-party firm can help make an assessment).

A potential advantage of promulgating an ethics standard such as IEEE 7000 or providing guidance and recommendations like ISO 26000 is that it provides engineers and product managers with a platform from which they might engage executives to raise concerns over safety and security. While senior executives ultimately might ignore recommendations from engineers, executives are not able to tell the employee/engineer that the concern raised is outside her professional domain precisely because it is based on a "standard" adopted by an engineering professional organization. The soft standards give the engineer a professionally grounded platform from which to raise safety and security concerns.

Corporate and engineering methods can also complement each other when focused on voluntary implementation of soft standards. This happens, for example, if management deemed it important to comply with ISO 26000 to demonstrate corporate social responsibility. A similar public relations goal might motivate compliance with IEEE 7000 for the ethical development of products using artificial intelligence. Engineers might assist with this process to ensure that marketing claims have a legitimate basis (avoiding liability for material misstatements and omissions or false advertising), even though the soft standards do not accommodate a verification and validation process which might be certified in the same manner as compliance with a conventional technical standard.

While traditional technical standards differ from soft standards, the most well-known "standard" applicable to automated vehicle technology, SAE J3016 (defining levels of performance of vehicle automation features), is not a standard at all. Rather, it is a collection of definitions used to discuss vehicle automation. Legislators and regulators sometimes use J3016 as if it defined meaningful levels of technology risk—but this is not the function of SAE J3016.

If a law uses technical definitions, such as the levels of automation features identified in SAE J3016, the matter is more complex. Engineering advice may assist with a determination that a product fits within a definitional category—thus furthering the oversight goal of compliance with law. In vehicle automation, a key issue for classification under J3016 is the design intent of an automation feature which engineers and product designers can confirm. However, this role can mask a deeper problem. In the case of J3016, the definitions were not created with a view to identifying levels of risk. For example, a Level 2 feature might be as dangerous, or more dangerous, in operation than a Level 3 feature. The legal regime uses these definitions at times as if the categories correspond to increasing levels of risk (i.e., by regulating Level 3 and above but not Level 2). Though engineering advice about compliance with law is appropriate, it should not distract engineers and product designers from the big-picture goal of developing a safe and secure product.

VII. Safety, Security, and Certification

Verification of compliance with technical specifications incorporated by reference may occur in various ways. A third party might certify compliance as occurs with the FCC-recognized Telecommunications Certification Bodies for devices that emit RF energy. A government agency may certify compliance as occurs in the case of the FAA's Aircraft Certification Service. Additionally, a private third party may provide a certification when not required by law such as Argo AI obtained from TÜV SÜD with respect to conformance with SAE J3018. In the weakest form of monitoring, a company may self-certify its own compliance with laws (e.g., FMVSS for automobiles)—a potentially dubious procedure if applied to certification of the safety of vehicle automation systems as evidenced by thinly sourced claims that an automation technology is safer than a human driver [23, 24].

In a regulatory process of certification, many certification steps may be approved by designees of a regulatory agency who, in fact, either are employees of companies or have significant relationships with companies. This presents a conflict of interest like that presented by pure self-certification. A board should establish and monitor a mechanism to address conflicts of interest for all the different forms of compliance certification and verification.

VIII. How Corporate and Engineering Goals Do Not Mesh

One objective of corporate governance is to limit the liability of members of the board of directors for breach of a fiduciary duty, including the duty of oversight. Avoiding liability does not require that the oversight be effective because the board of directors does not guarantee safety—but merely creates the conditions for development of safe and secure products, overseeing that managers use available resources to that end. In fact, ignorance sometimes provides a liability shield.

Engineering methods, in contrast, focus on designing a product that is, in fact, safe and secure, and otherwise meets the technical specifications as part of a verification process, as well as a validation process to confirm that a product is fit for purpose. When engineers provide the board with more detailed information, it may create liability for a failure by the board to act on that information. Moreover, the corporate governance obligation to maximize shareholder value may conflict with voluntary standards if compliance with the standard increases cost or delays series production.

A disconnect may exist between the public messaging from management about the technical capabilities of products and the perception of engineers as illustrated by press reports surrounding the Tesla recall and the progress of court cases brought by injured plaintiffs or their estates [25].

IX. Suggestions

Boeing's settlement for the 737 MAX derivative action can guide formation of corporate structures a board might use to facilitate development of safe and secure AI-driven products because its terms identify numerous connections between a corporate governance culture focused on safety and input from engineers. Other consent decrees (such as the

Cummins consent decree) and government publications used by the U.S. Department of Justice also can inform corporate structures useful to promote appropriate oversight [26].

Before the settlement (and in response to a lawsuit), Boeing created a dedicated Aerospace Safety Committee to oversee aircraft safety that was separate and apart from the prior risk management function in the audit committee—a structure that tragically failed. The settlement required this committee to consist of three or more independent directors with relevant engineering or safety experience. The settlement further required the separation of CEO from board chair and at least three directors with knowledge or expertise in aviation engineering or product safety oversight. The goal is to close a knowledge gap to permit informed oversight and to eliminate potential conflicts of interest.

The settlement required the Aerospace Safety Committee to meet when the board meets, and report results to the full board, with the Chief Aerospace Officer attending a board meeting twice a year, raising the profile of safety culture.

A Chief Aerospace Safety Officer and Chief Compliance Officer (though not required to regularly attend board meetings) had the task to ensure that each Aerospace Safety Committee meeting includes reporting and updates on significant safety issues, including new significant safety events. The settlement requires that briefing information be provided in sufficient detail so that the board members can understand management's judgments in developing safety policies and procedures, and in addressing significant safety events. These requirements formalize transfer of information from the bottom up to the board level. Required implementation of "Seek, Speak, Listen" programs, the creation of a "Speak Up" portal, and other communication channels further facilitate the transfer of information from the bottom-up to inform the board and its committees. This provides structure to a hybrid top-down, bottom-up management process.

The settlement required that executive compensation decisions include metrics related to safety to encourage strong oversight. Engineering input should inform safety metrics for automation—particularly in the absence of a mature regulatory environment which itself sets standards.

Not every organization has the size or resources to implement oversight mechanisms like Boeing. But surrogate structures might plug knowledge and responsibility gaps. At each board meeting, a technology safety and risk officer might report directly. The officer might be the chief engineer in charge of testing per Prof. Cummings' recommendation. Working with the legal department, the safety and risk officer might track compliance with technical laws, identifying relevant optional regulatory recommendations and standards to highlight with the board. Even without robust corporate structures, a board can learn about voluntary recommendations, standards, and best practices, as well as soft standards, related to AI and automation, and consult more general advice on corporate responsibility.

ACKNOWLEDGEMENTS

Dr. Wolf's work was supported in part by the NSF grant 2002854.

REFERENCES

[1] D. Shepardson, *Tesla recalls nearly all vehicles on US roads over lack of Autopilot safeguards*, REUTERS.COM, Dec. 13, 2023.

[2] G. Bensinger and D. Shepardson, *Exclusive: GM's Cruise robotaxi unit dismisses nine execs after safety probe*, REUTERS.COM, Dec. 13, 2023.

[3] B. Evans, *The 'AI doomers' have lost this battle*, FINANCIAL TIMES, Nov. 25, 2023.

[4] *See, e.g.*, Press Release, U.S. Dept. of Justice, Boeing Charged with 737 Max Fraud Conspiracy and Agrees to Pay over $2.5 Billion, Jan. 7, 2021 (noting that "Boeing's employees chose the path of profit over candor by concealing material information from the FAA").

[5] *In re* Caremark International Inc. Derivative Litigation, 698 A. 2d 959 (Del. Ch. 1996).

[6] MODEL BUS. CORP. ACT ANN. § 8.31(a)(2)(iv)(Am. Bar. Ass'n 2020).

[7] Firemen's Retirement System of St. Louis on behalf of Marriott International, Inc. v. Sorenson, 2021 WL 459377 (Del. Ch. 2022) (oversight requires ensuring risk management for cybersecurity).

[8] NIST Cybersecurity Framework 2.0. National Institute of Standards and Technology, Gaithersburg, MD. NIST Cybersecurity White Paper (CSWP) NIST CSWP 29 ipd, 2023.

[9] Artificial Intelligence Risk Management Framework (AI RMF 1.0) National Institute of Standards and Technology, Gaithersburg, MD, Jan. 2023.

[10] *In re* The Boeing Company Derivative Litigation, Stipulation and Agreement of Compromise, Settlement, and Release, Exhibit A: Corporate Governance Measures, Consol. C.A. No. 2019-0907-MTZ (Del. Ch. Nov. 5, 2021).

[11] *See, e.g.*, U.S. v. Cummins Inc., Consent Decree, Case 1:24-cv-00088 at 6 (D.D.C. Jan. 10, 2024).

[12] *See, e.g.*, B. Groysberg & M. Slind, *Leadership is a Conversation*, HARV. BUS. REV., June 2012 (observing reduced efficacy of traditional top-down management with new technologies).

[13] *In re* The Boeing Company Derivative Litigation, Memorandum Opinion, C.A. No. 2019-0907-MTZ, at 1 (Del. Ch. Sept. 7, 2021).

[14] Jack L. Marchand II v. John W. Barnhill, et al., C.A. No. 2017-0586-JRS (Del. 2019).

[15] M. Cummings, *Identifying AI Hazards and Responsibility Gaps*, in COMPUTER ETHICS ACROSS DISCIPLINES: APPLYING DEBORAH JOHNSON'S PHILOSOPHY TO ALGORITHMIC ACCOUNTABILITY AND AI (Noorman, M. E. & Verdiccio M., eds.) (Forthcoming 2024 in Springer Nature).

[16] *See, e.g.*, Teamsters Loc. 443 Health Servs. & Ins. Plan v. Chou, No. 2019-0816-SG (Del. Ch. Aug. 24, 2020).

[17] M. Anderljung, et al., Frontier AI Regulation: Managing Emerging Risks to Public Safety, arXiv:2307.03718v4 [cs.CY], Cornell, Nov. 7, 2023.

[18] *See* 5 U.S.C. § 552(a)(1) (providing that "matter reasonably available to the class of persons affected thereby is deemed published in the Federal Register when incorporated by reference").

[19] SEC Release, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure at p. 13.

[20] *See, e.g.*, S. Strother, *When Making Money is More Important Than Saving Lives: Revisiting the Ford Pinto Case*, 5 J. INT. & INTERDISCIPLINARY BUS. RESEARCH, 2018, p. 166.

[21] *See generally* P. KOOPMAN, HOW SAFE IS SAFE ENOUGH, 1st ed., 2022, pp. 193-195.

[22] *See* Nilsson v. Gen. Motors LLC, No. 18-471 (N.D. Cal. Jan. 22, 2018)(Answer and Demand for Jury Trial filed 3/30/18, Defenses and Affirmative Defenses. at 7, ¶ 2)(case settled before decision).

[23] M. Cummings & B. Bauchwitz, *Unreliable Pedestrian Detection and Driver Alerting in Intelligent Vehicles* [manuscript at 8], IEEE TRANSACTIONS ON INTELLIGENT VEHICLES, in press (questioning a regulatory approval process of self-certification).

[24] M. Cummings, "The search for transparent ADS safety metrics continues," Dec. 28, 2023, unpublished.

[25] R. Elliot and R. Felton, *Tesla's Engineers Are Less Boastful About Autopilot Than Elon Musk*, WALL ST. J., Dec. 15, 2023.

[26] *See, e.g.*, U.S. Dep't of Justice, Crimnal Division, Evaluation of Corporate Compliance Programs, updated Mar. 2023 (identifying features of well designed compliance programs).