INSURANCE COMPANIES AS CORPORATE REGULATORS: THE GOOD, THE BAD, AND THE UGLY

*Shauhin A. Talesh**

Introduction

Political scientists, economists, and legal scholars have been debating corporate social responsibility for decades.[1] To that end, the financial crisis, fraud relating to Enron and Worldcom, Occupy Wall Street, and even the 2016 presidential primary debates all raise attention and concern about what corporate social responsibility is and should be in the United States. The traditional view, the standard shareholder-oriented model, suggests "corporations have no specific social responsibilities beyond profit maximizing for the benefit of shareholders" as long as such profit maximizing occurs without violating the law or engaging in deception or collusion.[2] More recently, a progressive alternative, the stakeholder-oriented model, suggests corporate officers' and managers' underlying social obligations go beyond merely maximizing shareholders' wealth within the confines of following the law.[3] Rather, under this model, corporate social responsibility means that directors should consider the impact of their deci-

* Professor of Law, Director, Law & Graduate Studies Program, University of California, Irvine School of Law. I would like to thank Cathy Sharkey and Max Helveston for helpful comments on earlier drafts. I would also like to thank Itohan Okogbo and Elad Shem-Tov for outstanding research assistance on this project. An earlier version of this paper was presented in the spring of 2016 at the *22nd Annual Clifford Symposium of Tort Law and Social Policy* at DePaul University College of Law.

1. Henry N. Butler & Fred S. McChesney, *Why They Give at the Office: Shareholder Welfare and Corporate Philanthropy in the Contractual Theory of the Corporation*, 84 Cornell L. Rev. 1195, 1195 (1999) (noting the longstanding debate over corporate social responsibility).

2. Henry Hansmann & Reinier Kraakman, *The End of History for Corporate Law*, 89 Geo. L.J. 439, 440–41 (2001) (explaining the shareholder based model); Cynthia A. Williams, *Corporate Social Responsibility in an Era of Economic Globalization*, 35 U.C. Davis L. Rev. 705, 708 (2002).

3. *See* Steven M.H. Wallman, *The Proper Interpretation of Corporate Constituency Statutes and Formulation of Director Duties*, 21 Stetson L. Rev. 163, 168–70 (1991) (noting a more progressive approach toward corporate social responsibility). *See generally* Progressive Corporate Law (Lawrence E. Mitchell ed., 1995); Frank Partnoy, *Adding Derivatives to the Corporate Law Mix*, 34 Ga. L. Rev. 599 (2000).

sions on a wider range of constituents, including employees, consumers, suppliers, the community, and the environment.[4]

To whom the corporation is responsible is juxtaposed against the reality that corporations are subject to more laws and regulations than ever before. Modern corporations are subject to an expansive set of laws through the legal acts of incorporation, bankruptcy, mergers, acquisitions, patent, copyright, antitrust, health and safety, labor, employment, and environmental laws. Laws attempt to guide, impact, and constrain corporations as they operate.

Despite a wide variety of laws pressing on corporations, it is less clear how legal regulations influence corporate social responsibility. Laws regulating the behavior of organizations are often ambiguous and vague with respect to how to comply.[5] Moreover, many of the laws regulating organizations are complex and require elevated levels of expertise. It is not entirely clear how legal regulation shapes not only the internal governance of a corporation, but also assures corporations comply with labor and employment, environmental, privacy, and financial regulation and securities laws. Thus, despite the plethora of laws impacting corporations, there remains an ongoing debate concerning the best way to regulate corporations, especially given that approaches anchored in private contract law are insufficient.

Prior research focuses on the role regulatory intermediaries play in assisting organizations to comply with various laws.[6] These approaches suggest that despite the vast array of laws imposed on corporate entities, legal and non-legal actors within or affiliated with organizations play a significant role in shaping the way organizations go about complying with laws. These regulatory intermediaries consist of corporate actors such as directors and officers as well as corpo-

---

4. *See* Wallman, *supra* note 3, at 168–70; *see also* David Millon, *Communitarianism in Corporate Law*, *in* PROGRESSIVE CORPORATE LAW, *supra* note 3, at 11–12; Partnoy, *supra* note 3, at 609–10.

5. *See* Shauhin Talesh, *A New Institutional Theory of Insurance*, 5 U.C. IRVINE L. REV. 617, 621–22 (2015). "[T]here is nearly always some degree of legal ambiguity in laws regulating organizations." *Id.* (citing Lauren B. Edelman, *Legal Ambiguity in Symbolic Structures: Organizational, Mediation of Civil Rights Law*, 97 AM. J. SOC. 1531–38 (1992)). "This ambiguity in legal regulation leaves a space for the social construction of the meaning of law . . . ." *Id.* (citing Lauren B. Edelman, *Overlapping Fields and Constructed Legalities: The Endogeneity of Law*, *in* PRIVATE EQUITY, CORPORATE GOVERNANCE AND THE DYNAMICS OF CAPITAL MARKET REGULATION 55, 58–65 (Justin O'Brien ed., 2007)).

6. For a summary of the ways that intermediaries impact and influence the way organizations respond to law, see Shauhin Talesh, *Legal Intermediaries: How Insurance Companies Construct the Meaning of Compliance with Antidiscrimination Laws*, 37 L. & POL'Y 209, 212–14 (2015); Shauhin A. Talesh, *Rule-Intermediaries in Action: How State and Business Stakeholders Influence the Meaning of Consumer Rights in Regulatory Governance Arrangements*, 37 L. & POL'Y 1, 24–25 (2015).

rate-affiliated actors like in-house counsel, managers, and human resource officials. Intermediaries try to advise, interpret, and implement laws in ways that attempt to achieve compliance. Legal intermediaries play a major role in shaping the content and meaning of laws designed to regulate corporations, how corporations understand law and compliance, and how corporations go about responding to laws.

This Article explores an intermediary of corporate behavior that has been less explored by corporation and organizational behavior scholars: insurance companies. In recent years, insurers are increasingly acting as corporate regulators. Prior research in insurance law suggests that insurance acts as a substitute for regulation and highlights the ways insurance institutions act as risk regulators and regulate so many aspects of an individual's and organization's relationships in society.[7] Scholars suggest that insurance can serve as a substitute for regulation and monitor organizational behavior in ways the government does not. These scholars are largely optimistic about insurance as a substitute for regulation[8] and the role of insurance companies as risk managers of corporate responses to regulation.[9] However, there has been less empirical inquiry into the precise role of insurance companies as regulators of corporations. In particular, how and under what conditions do insurance companies regulate corporate behavior and influence corporate social responsibility? Corporations are subject to more laws and are interconnected with more constituents and shareholders than ever before. This Article addresses how insurance companies regulate corporate behavior. In order to explore how corporations impact the wide variety of constituents and stakeholders that go beyond shareholders, I examine corporate behavior from a stakeholder perspective.

Drawing from empirical research of insurance companies that advise corporations on how to comply with privacy, securities, and employment laws, this Article argues that the value of insurance and insurance institutions as substitutes for regulation is not as uniformly

---

7. *See* Omri Ben-Shahar & Kyle D. Logue, *Outsourcing Regulation: How Insurance Reduces Moral Hazard*, 111 MICH. L. REV. 197, 217–28 (2012) (arguing insurance acts a form of risk regulation and performs regulatory functions better than government in many instances). For a comprehensive explanation of the concept of insurance as regulation, see *infra* notes 29–46 and accompanying text.

8. *See* Ben-Shahar & Logue, *Outsourcing Regulation*, *supra* note 7, at 199–200 (arguing insurance regulates safety better than the government and can reduce and solve moral hazard and other incentive problems).

9. *Id.* at 228, 235–38 (highlighting why insurers are potentially better regulators than government).

positive as previously suggested. In particular, insurance companies are not simply pooling and transferring risk. Rather, insurers are using their risk management tools and services to influence how corporations comply with laws. This Article argues that insurance company interventions range from positive (good) to negative (bad) to downright ugly (i.e., insurer interventions have unappealing impacts on the way organizations understand their legal obligations). With my focus on qualitative case studies of insurer risk management techniques in action, I highlight the specific ways insurers facilitate and inhibit compliance with law and corporate social responsibility in different situations.

This Article proceeds as follows: Part II briefly articulates the various strands of corporate social responsibility, noting that little attention is paid to focusing on the role of insurance companies as corporate regulators.[10] I then examine insurance law scholarship, which focuses on how insurance acts as a substitute for regulation. Part II concludes by noting that these scholars have largely celebrated the role of insurers as risk managers without close exploration of the processes and mechanisms through which insurers act as risk regulators.

Part III uses three case studies to explore how insurance companies act as regulators of corporate behavior with respect to privacy, securities, and employment law.[11] I argue that empirical research in this area suggests that insurers as corporate regulators is a mixed bag: sometimes good, sometimes bad, and sometimes unappealing.

In response to the rise in data breach events and the accompanying privacy laws, insurers are now offering organizations cyber insurance. My empirical research reveals that insurers absorb many of the responsibilities of an organization's legal, compliance, public relations, and information technology departments by offering risk management services to prevent and detect data breaches before they occur. Given that organizations are admittedly under-prepared for data breach events and under-compliant with privacy laws, I conclude that insurance company risk management interventions have been largely helpful.[12]

After highlighting the relatively positive risk management approaches used by insurers, I then highlight the negatives of insurer risk management. Unlike in the cyber insurance context, insurance companies offering directors' and officers' insurance have opportuni-

10. *See infra* notes 16–46 and accompanying text.
11. *See infra* notes 47–153 and accompanying text.
12. *See infra* notes 47–96 and accompanying text.

ties to engage in loss prevention and discourage wrongful or even illegal behavior, but fail to do so. Insurance companies acting as corporate regulators in this instance do little more than ensure corporate misconduct and undermine shareholder litigation.[13]

My final case study explores how insurers in the past twenty years have begun offering employment practice liability insurance. This is insurance for employers sued for sexual harassment, wrongful termination, and other employment violations. Unlike the directors' and officers' insurers that had opportunities to engage in loss prevention but failed to do so, I find that employment practice liability insurers' do offer risk management and loss prevention advice but do so in a way that weakens the meaning of antidiscrimination law. Thus, insurance company regulatory intervention in the employment law context may help employers avoid being sued, but may have some perverse and unappealing effects as well.[14]

This Article, therefore, contributes to studies of corporate social responsibility and insurance. First, I shine light on a different professional intermediary that is less explored by those interested in the way professional intermediaries impact corporate social responsibility. Second, this Article contributes to insurance-as-regulation literature by using prevailing empirical research on insurers as risk managers to show under what conditions insurance risk management facilities or inhibits corporate compliance with laws. Recent scholarship suggests insurance substitutes as regulation in positive ways, but my empirical lens presents a more complex picture. I show that insurance-as-regulation goes beyond deterrence and loss prevention and reducing moral hazard. Insurance institutions *transform* the meaning of compliance and the deterrence signal.

I conclude by suggesting that the insurance-as-regulation narrative previously articulated by scholars requires more nuance and empirical exploration.[15] The debate going forward is not whether insurers are good risk regulators as prior scholars theorize, but more precisely, examining under what conditions can insurers make positive regulatory interventions into corporate behavior and nudge corporations toward a governance structure in line with societal values of fairness, equality, transparency, and safety. From a public policy standpoint and consistent with the stakeholder model of corporate social responsibility, I conclude that we should not defer to insurer intermediary practices

13. *See infra* notes 97–122 and accompanying text.

14. *See infra* notes 123–53 and accompanying text.

15. *See infra* notes 154–55 and accompanying text.

without seeing tangible evidence that such responses are in fact working well and leading to greater compliance by corporations.

II. The Role of Private Insurance Companies as Substitutes for Public Regulation

Corporate social responsibility suggests that business and society are interwoven. What corporate social responsibility means and who the corporation is ultimately beholden to has been debated for decades. I will not try to summarize the vast literature in this Article but, instead, point out the two dominant ways that scholars conceptualize corporate responsibility. The standard shareholder-oriented model suggests corporate managers are charged with managing the corporation exclusively in the shareholders' economic and profit-maximizing interests.[16] This approach suggests the interests of other corporate stakeholders, such as creditors, suppliers, employees and customers, are protected[17] by other laws, such as antitrust, consumer protection, labor, employment, privacy, and environmental law.[18] Other constituents find protection in explicit contracts with the corporation.

The progressive alternative is derived from the stakeholder theory of the corporation. This model suggests that corporate managers' social obligations include considering the impact of their decisions on a wider range of constituents than shareholders, including employees, consumers, suppliers, and the environment.[19] Corporations have responsibilities to the larger community because of their role as economic institutions and their impact on society.[20] Public laws and regulations and private contract law try to protect the interests of employees, consumers, and the environment more broadly.[21]

---

16. *See* Hansmann & Kraakman, *supra* note 2, at 440–41 (2001); *see also* Milton Friedman, Capitalism and Freedom 133 (1962); Milton Friedman, *The Social Responsibility of Business Is to Increase Its Profits*, N.Y. Times Mag., Sept. 13, 1970, at 32–33.

17. Hansmann & Kraakman, *supra* note 2, at 442.

18. *See* Williams, *supra* note 2, at 713 ("While Hansmann and Kraakman recognize corporate responsibilities to constituents other than shareholders, where those responsibilities are embodied in positive law (such as in antitrust, consumer protection, labor, or environmental laws) or in explicit contracts, and they recognize the importance of corporations serving the interests of society as a whole, they reject the view that corporate law itself ought to embody a multi-fiduciary or stakeholder model of accountability." (footnotes omitted)).

19. Wallman, *supra* note 3, at 170.

20. *See* Ronen Shamir, *Capitalism, Governance, and Authority: The Case of Corporate Social Responsibility*, 6 Ann. Rev. L. & Soc. Sci. 531, 532–53 (2010).

21. *See* Williams, *supra* note 2, at 720 (noting that formal legal rules have not protected most constituencies).

Under either framework, laws that impact organizations are supposed to press down on organizations and force them to comply with legal regulations. Thus, in theory, law is supposed to play a big role in protecting shareholders and other stakeholder rights when dealing with organizations. In fact, there are plenty of laws regulating various aspects of organizations. In particular, employment and anti-discrimination law attempt to protect the rights of employees to work in a discrimination free workplace. Privacy laws require organizations to notify consumers in the event of a data breach. Consumer protection laws seek to protect consumers in transactions with businesses. Securities laws seek to protect shareholders from scrupulous corporate practices. Environmental laws require organizations to conduct their business in ways that do not pollute or harm the environment. Of course, these laws are just a few of the many laws impacting organizations. Given the multitude of laws regulating organizations and the lack of clarity in many laws with respect to how to comply with them, I have previously explored how corporations often shape and influence the content and meaning of the legislation and regulatory rules that are designed to regulate them.[22] Moreover, in trying to interpret and implement various laws that organizations are subject to, organizations frequently look to managers, in-house counsel, and other professionals to help achieve compliance with these laws.[23]

Prior research that explores how organizations respond to law shows that business, management, and legal professionals are key carriers of ideas among and across organizations. In particular, human resource officials, personnel managers, management consultants, and in-house lawyers communicate ideas about law as they move among organizations, participate in conferences, workshops, training sessions, professional networking meetings, and publish professional personnel

22. For further conceptualization of how private organizations shape the content and meaning of laws that are designed to regulate them, see generally LAUREN EDELMAN, WORKING LAW: COURTS, CORPORATIONS & SYMBOLIC CIVIL RIGHTS (2016); Lauren B. Edelman & Shauhin A. Talesh, *To Comply or Not to Comply—That Isn't the Question: How Organizations Construct the Meaning of Compliance*, *in* EXPLAINING COMPLIANCE: BUSINESS RESPONSES TO REGULATION 103 (Christine Parker & Vibeke Lehmann Nielsen eds., 2011); Shauhin A. Talesh, *How Dispute Resolution System Design Matters: An Organizational Analysis of Dispute Resolution Structures and Consumer Lemon Laws*, 46 L. & SOC'Y REV. 463 (2012); Shauhin A. Talesh, *Institutional and Political Sources of Legislative Change: Explaining How Private Organizations Influence the Form and Content of Consumer Protection Legislation*, 39 L. & SOC. INQUIRY 973 (2014); Shauhin A. Talesh, *The Privatization of Public Legal Rights: How Manufacturers Construct the Meaning of Consumer Law*, 43 L. & SOC'Y REV. 527 (2009).

23. Given that different scholarly communities use the terms corporations and organizations, I will use the term interchangeably.

literature.[24] Existing empirical research reveals that when organizations attempt to comply with laws, managerial conceptions of law broaden the term "diversity" in a way that disassociates it from its original goal of protecting civil rights,[25] transform sexual harassment claims into personality conflicts,[26] deflect or discourage complaints rather than offering informal resolution,[27] and even shape the way arbitrators understand law and compliance.[28] Thus, we know corporations are subject to complying with a vast array of laws, have multiple constituencies beyond their shareholders, and increasingly look to professional intermediaries on how to comply with laws.

More recently, insurance scholars are discussing the role of insurance as a form of regulation over individuals and organizations.[29] Insurance regulates many aspects of our lives. Insurance companies establish the underwriting criteria and standards and charge premiums based on various risk-profiles. These mechanisms allow insurance companies to control who can or cannot obtain insurance.[30] Through insurance policy terms and pricing provisions, insurance companies

---

24. For a series of studies highlighting how the professions mediate and managerialize law, see generally SANFORD M. JACOBY, EMPLOYING BUREAUCRACY: MANAGERS, UNIONS, AND THE TRANSFORMATION OF WORK IN AMERICAN INDUSTRY, 1900–1945 (1985); James N. Baron et al., *War and Peace: The Evolution of Modern Personnel Administration in U.S. Industry*, 92 AM. J. SOC. 350 (1986); Lauren B. Edelman et al., *Diversity Rhetoric and the Managerialization of Law*, 106 AM. J. SOC. 1589, 1594–99 (2001); Lauren B. Edelman et al., *Internal Dispute Resolution: The Transformation of Civil Rights in the Workplace*, 27 L. & SOC'Y REV. 497, 505–06, 514–15 (1993); Talesh, *Legal Intermediaries*, *supra* note 6, at 210, 226–34.

25. *See* Edelman et al., *Diversity Rhetoric*, *supra* note 24, at 1590 (examining how managerial rhetoric about diversity influences employers' employment policies and procedures and how professional personnel literature broadens how the term "diversity" is used in relation to discrimination claims).

26. *See* Edelman et al., *Internal Dispute Resolution*, *supra* note 24, at 516–17 (showing how grievance and anti-harassment officers transform legal disputes into interpersonal disputes and focus on healing the relationship).

27. *See* Anna-Maria Marshall, *Idle Rights: Employees' Rights Consciousness and the Construction of Sexual Harassment Policies*, 39 L. & SOC'Y REV. 83, 85–86 (2005) (showing how sexual harassment policies are constructed through a managerial lens).

28. *See* Talesh, *Dispute Resolution*, *supra* note 22, at 469 ("[L]aw becomes 'managerialized' when business values such as rationality, efficiency, and management discretion operating within an organizational field influence the way organizations understand law, legality, and compliance.").

29. For a comprehensive explanation of the concept of insurance as regulation, see generally Shauhin A. Talesh, *Insurance and the Law*, *in* INTERNATIONAL ENCYCLOPEDIA OF SOCIAL & BEHAVIORAL SCIENCES 215 (James D. Wright ed., 2d ed. 2015); Tom Baker, *Insurance in Sociolegal Research*, 6 ANN. REV. L. & SOC. SCI. 433 (2001) [hereinafter *Sociolegal Research*]; Tom Baker, *Liability Insurance as Tort Regulation: Six Ways that Liability Insurance Shapes Tort Law in Action*, 12 CONN. INS. L.J. 1, 10–12 (2005); Omri Ben-Shahar & Kyle D. Logue, *How Insurance Substitutes for Regulation*, REGULATION, Spring 2013, at 36 [hereinafter *Substitutes for Regulation*]; Ben-Shahar & Logue, *Outsourcing Regulation*, *supra* note 7.

30. *See* Ben-Shahar & Logue, *Substitutes for Regulation*, *supra* note 29, at 37–41.

also establish norms of conduct. Private insurance policies for life, health, and property often take the form of private legislation or regulation through a wide variety of exclusions and conditions. In addition to serving a gatekeeping function, liability insurance acts as a form of tort regulation and, in doing so, finances the civil litigation system.[31]

Although many commentators note that insurance companies often act as regulators of risk,[32] Professors Omri Ben-Shahar and Kyle Logue argue that insurance companies have advantages as regulators over the government due to information and motivation asymmetries. In drawing a distinction between government regulators and insurers, these scholars note that government regulators are not paid for performance, lack adequate incentives, are not disciplined by market forces, and lack advanced tools for information acquisition, aggregation, and prediction.[33] Through actuarial techniques, private contracting, and ex post claim investigation, Ben-Shahar and Logue argue insurers do not only engage in risk regulation, but insurers can also reduce insureds' moral hazard behavior and induce efficient risk-reducing behavior in ways that government regulators fail or have limited success.[34] In particular, they argue that insurance develops templates to regulate behavior in ways that are potentially more precise than some forms of governmental control.[35] Moreover, even when government is needed to regulate when insurance markets fail, insurers provide the necessary information and motivation to nudge

---

31. *See* Baker, *Liability Insurance*, *supra* note 29, at 13 (2005) ("[L]iability insurance is a de facto element of tort law" and a de facto cap on tort damages). *See generally* KENNETH S. ABRAHAM, THE LIABILITY CENTURY: INSURANCE AND TORT LAW FROM THE PROGRESSIVE ERA TO 9/11 (2008) (exploring how both first-party and third-party liability insurance influenced the development of tort liability); Stephen C. Yeazell, *Re-Financing Civil Litigation*, 51 DEPAUL L. REV. 183 (2001) (highlighting how insurance and credit finance the civil litigation system).

32. *See* KENNETH S. ABRAHAM, DISTRIBUTING RISK: INSURANCE, LEGAL THEORY, AND PUBLIC POLICY 57 (1986) (noting "surrogate regulation" when describing the new regulatory role being imposed on liability insurers to regulate toxic tort and environmental risks); DAVID A. MOSS, WHEN ALL ELSE FAILS: GOVERNMENT AS THE ULTIMATE RISK MANAGER 10 (2002); Tom Baker, *Bonded Import Safety Warranties*, *in* IMPORT SAFETY: REGULATORY GOVERNANCE IN THE GLOBAL ECONOMY 215, 216–22 (Cary Coglianese et al. eds., 2009) (advocating for reliance on insurers to police food safety); Jon D. Hanson & Kyle D. Logue, *First-Party Insurance Externality: An Economic Justification for Enterprise Liability*, 76 CORNELL L. REV. 129, 188 (1990) (calling for moving the regulatory function of product safety to products-liability insurers through adoption of strict products liability); Joshua Ronen, *Post-Enron Reform: Financial-Statement Insurance and GAAP Revisited*, 8 STAN. J.L. BUS. & FIN. 39, 48–60 (2002) (arguing for using insurance to regulate the accuracy of financial statements).

33. Ben-Shahar & Logue, *Outsourcing Regulation*, *supra* note 7, at 198–99 (noting the problems with government regulators and arguing that insurers can outperform government regulators).

34. *Id.* at 199–229 (highlighting how insurers act as risk regulators).

35. *Id.*

government regulators to act.[36] Thus, under this approach, insurers' loss prevention tools can enhance tort law's deterrent effects.[37] Insurers have the power to regulate in a variety of ways, including "mandating specific investments in risk reduction, offering premium discounts for favorable claims experience, to selling cost-containment expertise to policyholders and even designing safety technologies and codes."[38] In addition, insurers use private contracting as a mechanism for monitoring organizational behavior and compliance.

Focusing on policy language, actuarial, and underwriting practices, these scholars argue that insurance covering product liability, workers' compensation, automobiles, homeowners, environmental liability, and tax liability, regulate individuals and businesses in ways that are more constructive than government regulation.[39] In particular, because insurers have superior access to information and commercial sophistication, they deploy a series of strategies to improve the safety conduct of their policyholders. Ben-Shahar and Logue conclude that because of insurers' inherent informational advantage, these institutions are better regulators than regulatory, legislative, or judicial institutions.[40] Other scholars have explored the relationship between loss prevention and policyholder moral hazard across a variety of domains including legal malpractice,[41] medical malpractice,[42] motion pictures,[43]

36. *Id.*

37. *See* Abraham, The Liability Century, *supra* note 31, at 228 (recognizing that "a version of tort law's deterrence function has slowly been incorporated into insurance"); Catherine M. Sharkey, *Revisiting the Noninsurable Costs of Accidents*, 64 Md. L. Rev. 409, 413 (2005) ("Insurance companies, as private regulators, are well positioned to achieve deterrence through experience rating of firms and other actors, as well as by providing risk management services."); Steven Shavell, *On Liability and Insurance*, 13 Bell J. Econ. 120, 120–21 (1982) (arguing that when certain assumptions are taken into account, liability insurance is socially desirable).

38. Ben-Shahar & Logue, *Outsourcing Regulation*, *supra* note 7, at 247.

39. *Id.* at 217–28 (highlighting how insurance as risk regulator works better than the government).

40. *Id.* at 201 ("We contend that private insurance markets can and sometimes do outperform the government in regulating conduct because of both superior information and competition.").

41. *See generally* George M. Cohen, *Legal Malpractice Insurance and Loss Prevention: A Comparative Analysis of Economic Institutions*, 4 Conn. Ins. L.J. 305 (1997); Anthony E. Davis, *Professional Liability Insurers as Regulators of Law Practice*, 65 Fordham L. Rev. 209 (1996).

42. *See generally* Katherine Baicker & Amitabh Chandra, *The Effect of Malpractice Liability on the Delivery of Health Care*, F. Health Econ. & Pol'y, Jan. 2005, at 1; Tom Baker, *Medical Malpractice and the Insurance Underwriting Cycle*, 54 DePaul L. Rev. 393 (2005); Bernard Black et al., *Stability, Not Crisis: Medical Malpractice Claim Outcomes in Texas*, 1988-2002, 2 J. Empirical Legal Stud. 207 (2005).

43. *See generally* Elizabeth O. Hubbart, *When Worlds Collide: The Intersection of Insurance and Motion Pictures*, 3 Conn. Ins. L.J. 267 (1997).

firearms,[44] personal injury,[45] and most recently policing.[46] Thus, across a variety of areas, insurers regulate corporations. Because corporations impact a wide variety of constituents such as shareholders, employees, and suppliers, as the shareholder theory of corporate social responsibility suggests and are subject to a wide variety of laws, insurance and insurance companies in particular, play a major role in trying to assure corporate social responsibility, within the shareholder and stakeholder models of corporate social responsibility.

As insightful as this work and that of others who discuss insurance as a form of regulation is, studies in this area focus primarily on insurance policy provisions, actuarial techniques, and claims practices as generating a form of regulatory oversight. Rarely is there a strong focus on the role that insurance companies play. Finally, and most importantly, there is little empirical research designed to uncover the processes and mechanisms through which insurers engage in risk regulation. *How* do insurers as risk regulators work in action? Does it always work? *Under what conditions* does insurance as a form of regulation work? Despite the well-settled belief in the field that insurers act as risk regulators and that insurers are a welcome substitute to government, there is little fine-grained analysis of how insurance companies go about acting as regulators. To the extent that insurers are regulatory intermediaries, there is less data on how this occurs and what the benefits and burdens of such an approach are.

The following attempts to address this void by examining how insurers go about regulating organizations. In particular, this Article uses three case studies to explore this question: under what conditions do insurance companies act as risk regulators? It also explores the impact of insurer interventions through risk management programs that they offer organizations. In particular, this Article focuses on how insurers do not just engage in risk regulation, but often shape and influence the meaning of compliance among corporations in good, bad, and sometimes unappealing ways. Given that corporations who care about corporate social responsibility often look to insurers as potential intermediaries, the following case studies provide a closer analysis of the ways in which insurers facilitate or hinder corporate social re-

44. *See generally* Tom Baker & Thomas O. Farrish, *Liability Insurance & the Regulation of Firearms*, *in* SUING THE GUN INDUSTRY: A BATTLE AT THE CROSSROADS OF GUN CONTROL AND MASS TORTS 292 (Timothy D. Lytton ed., 2005).

45. *See generally* STEPHEN D. SUGARMAN, DOING AWAY WITH PERSONAL INJURY LAW: NEW COMPENSATION MECHANISMS FOR VICTIMS, CONSUMERS, AND BUSINESS (1989).

46. *See generally* John Rappaport, *How Private Insurers Regulate Public Police*, 130 HARV. L. REV. 1539 (2017) (arguing insurance risk management encourages better policing practices).

sponsibility and compliance with the vast array of laws that corporations are subject to complying with.

III. Empirical Perspectives on Insurance Companies as Corporate Regulators

A. *Insurance Risk Management in the Privacy and Data Breach Context: The Good*

Cybersecurity risks (i.e., "loss exposure associated with the use of electronic equipment, computers, information technology, and virtual reality") are among the biggest new threats facing businesses and most consumers.[47] Data breach events cause financial and public relations damage and threaten an organization's survival.[48] Organizations also face compliance challenges as they are forced to navigate between the various federal and state laws and regulations concerning the collection and use of personal data. Despite these threats, prevailing empirical research suggests private organizations are not significantly changing their behavior. Although many organizations do have formal policies in place, the majority of organizations do not believe that they are sufficiently prepared for a data breach, do not devote adequate money, training, and resources toward protecting consumer's electronic information from data breaches, and fail to perform proper risk assessments.[49] In fact, many organizations find

---

47. Gregory D. Podolak, *Insurance for Cyber Risks: A Comprehensive Analysis of the Evolving Exposure, Today's Litigation, and Tomorrow's Challenges*, 33 QUINNIPIAC L. REV. 369, 371 (2015) (quoting Gregory D. Podolak, *Cyber Risk Coverage Litigation Heats Up as Exposure and the Insurance Market Evolve*, A.B.A. INS. COVERAGE LITIG. (June 13, 2014), http://apps.americanbar.org/litigation/committees/insurance/articles/marchapril2014-cyber-risk-litigation.html) (discussing the surge in cyber risks in society across all aspects of society).

48. *See* Roberta D. Anderson, *Viruses, Trojans and Spyware, Oh My! The Yellow Brick Road to Coverage in the Land of Internet Oz*, 49 TORT TRIAL & INS. PRAC. L.J. 529, 530–42 (2014) (discussing data breach impact in terms of costs, reputation, and organizations' survival); Podolak, *Insurance for Cyber Risks*, *supra* note 47, at 371–75.

49. *See* PONEMON INST., FIFTH ANNUAL BENCHMARK STUDY ON PRIVACY & SECURITY OF HEALTHCARE DATA 1 (2015), https://media.scmagazine.com/documents/121/healthcare_privacy_security_be_30019.pdf ("[M]ajority of healthcare organizations represented in this study have experienced multiple security incidents and nearly all have faced a data breach. Despite the universal risk for data breach, the study found that many organizations lack the funds and resources to protect patient data and are unprepared to meet the changing cyber threat environment."); *see also HSB Study Shows 69 Percent of Businesses Experienced Hacking Incidents in the Last Year*, BUS. WIRE (June 3, 2015, 11:39 AM) [hereinafter *HSB Study Shows*], http://www.businesswire.com/news/home/20150603006200/en/HSB-Study-Shows-69-Percent-Businesses-Experienced ("[M]ore than half (55 percent) don't believe their company is dedicating enough money or trained and experienced personnel to combat the latest hacking techniques.").

complying with multiple security frameworks difficult, time-consuming, and expensive.[50]

Recognizing this under-preparation and under-compliance gap, the insurance field stepped in and, in the last decade, began offering cyber insurance. Cyber insurance is insurance designed to provide both first-party loss and third-party liability coverage for data breach events, privacy violations, and cyberattacks.[51] Although there is variation in the types of policies being offered, insurers offering cyber insurance provide some risk shifting for the costs associated with having to respond, investigate, defend, and mitigate against the consequences surrounding a data breach event, cyberattack, and privacy violation.[52] Organizations are increasingly purchasing cyber insurance to deal these new risks.[53]

Insurance companies and institutions, through cyber liability insurance, do not simply pool and transfer an insured's risk to an insurance company or provide defense and indemnification services to an insured. In addition to transferring risk, my empirical research suggests that cyber insurance provides a series of risk management services that actively shape the way an organization's various departments tasked with dealing with data breach, such as in-house counsel, information technology, compliance, public relations, and other organizational units, respond to data breach. Cyber insurers are acting as compliance regulators and trying to prevent, detect, and respond to data breaches and help organizations comply with various privacy laws. Thus, cyber insurers frame the legal environment in terms of

50. Taylor Armerding, *'Compliance Fatigue' Sets In*, CSO ONLINE (Mar. 20, 2015, 7:44 AM), http:// www.csoonline.com/article/2899612/compliance/compliance-fatigue-sets-in.html (discussing how compliance with multiple security frameworks is difficult, time-consuming, and expensive).

51. *See* Amy Elizabeth Stewart, *Insurance Law Update: It's Not Just the Other Guy*, 70 ADVOC. (TEX.) 248, 257–58 (2015) (explaining the basic features of cyber insurance). *See generally* William T. Um, *Is Cyberinsurance the New 'Must Have' Policy?*, L.A. DAILY J., Nov. 12, 2014.

52. *Id.*

53. Whereas most companies did not have cyber insurance a decade ago, one in three organizations now have insurance specifically protecting against cyber and data theft losses. Deirdre Fernandes, *More Firms Buying Insurance for Data Breaches*, BOS. GLOBE (Feb. 17, 2014), www.bostonglobe.com/business/2014/02/07. In 2013, cyber insurance policies sold to retailers, hospitals, banks, and other businesses rose 20% according to Marsh LLC, a New York insurance brokerage firm that tracks the market. *Id. See generally HSB Study Shows*, *supra* note 49. The United States cyber insurance market is approximately 90% of the global market, with annual gross written premiums estimated around 2 billion for 2014 and 1.3 billion in 2013. Stephane Hurtaud et al., *Cyber Insurance as One Element of the Cyber Risk Management Strategy*, INSIDE, Jan. 2015, at 92–97.

risk and then encourage corporations to use their risk management services to avoid data breaches and privacy law violations.[54]

Drawing from interviews and participant observation at cyber insurance conferences across the country and content analysis of cyber insurance policies, loss prevention manuals, cyber insurance risk management services, and webinars, I conducted an empirical study that reveals that insurers absorb many of the responsibilities of an organization's information technology department with risk management services that they offer and try to prevent and detect data breaches before they occur.[55] Many of the issues that arise during a data breach that are often handled by internal departments within an organization, such as legal, compliance, information technology and public relations/crisis management, are now being assisted and guided by insurance industry professionals or third-party vendors that insurance companies offer to assist organizations at a reduced fee.[56] Cyber insurance provides a pathway for insurance institutions to act as external compliance monitors and managers of organizational behavior with respect to data theft. Given the under-preparation and under-compliance by businesses, institutionalized risk management techniques developed within the insurance field can potentially improve organizational practices and compliance concerning data breach.[57]

Before diving into the risk management tools and tactics that insurers use to assist organizations with complying with privacy laws and preventing data breach events, it is important to acknowledge that cyber policies are somewhat different than other insurance lines. Cyber insurers are able to position themselves as regulatory in-

54. Cyber insurer risk framing of the legal environment of corporations is consistent with how the insurance field frames the legal environment of employers. *See* Talesh, *Legal Intermediaries*, *supra* note 6, at 210–31 (showing how the insurance field frames the legal environment in terms of risk).

55. For a more elaborate analysis of the empirical study that I conducted, see Shauhin Talesh, *Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses*, L. & Soc. Inquiry doi:10.1111/lsi.12303 (2017).

56. *Id.* at 9–19; *see* David L. Hudson, Jr., *Cyber Liability Insurance Is an Increasingly Popular, Almost Necessary Choice for Law Firms*, A.B.A. L.J. (Apr. 1, 2015, 3:20 AM), http://www.abajournal.com/magazine/article/cyber_liability_insurance_is_increasingly_popular_almost_necessary_choice ("'[S]ome carriers go beyond just offering an insurance policy and also offer risk management services which firms can use to further protect against these exposures. These services can actually be quite robust and innovative. Finally, insureds are able to tap into a built-in network of IT experts, PR firms and legal counsel experienced in cyber matters, which brings an enormous amount of value to the coverage.' Most carriers 'offer a menu of coverages which can be selected depending upon an insured's specific needs.'" (quoting Chris Andrews, Vice President, Professional Liability, AIG)).

57. *Id.* (arguing that insurer risk management in this context is less about shaping law and more about protecting the corporation from data breach).

termediaries by offering expansive coverage for privacy and data breach violations where property, commercial general liability, errors and omissions, and other lines of insurance often exclude coverage.[58] Moreover, unlike some lines of insurance, cyber insurance provides both first and third-party coverage for data breach events, privacy violations, and cyber-attacks.[59] Cyber insurance covers the insured when the organization experiences a data breach but also obtains coverage for liability to others such as consumers to whom the insured is liable to. Cyber insurance also covers the costs that flow from a data breach, including the costs to notify and monitor the credit of the victims, perform a forensic investigation, and handle the public relations campaign to maintain and restore the public's trust in the organization.[60]

Insurance companies do not just influence organizations through the policies they issue. Insurers do more. Insurance companies offering cyber insurance influence how organizations comply with privacy laws and deal with data breach events through a variety of risk management services. The risk management services are aimed at preventing, detecting, and responding to data breach. My fieldwork revealed that the insurance industry and the private organizations purchasing this insurance were in "partnership" with one another.[61] One of the reasons organizations purchase this insurance is to gain access to the insurance company vendor's that assist with helping prevent, detect, and respond to data breach.[62] Seventy percent of the panels that I attended and observed at cyber insurance conferences mentioned or promoted the value of the risk management services that accompany cyber policies.[63] Thus, cyber insurance and the accompanying risk management services that come with the insurance provide a pathway for insurance companies to influence organizational decision-making and response concerning cybersecurity compliance issues.

58. *See* Hurtaud et al., *supra* note 53, at 95 fig.2 (highlighting how cyber coverage provides coverage for a series of risks that other lines of insurance occasionally cover).

59. *See* Anderson, *supra* note 48, at 529, 591–607. *See generally* Hurtaud et al., *supra* note 53; Um, *supra* note 51. I should be clear that cyber insurance is not the only line of insurance to offer both first and third-party insurance. For example, homeowners and auto insurance also offer first and third-party insurance. However, many other lines of insurance offer either first or third. Thus, insurers that package first and third-party coverage together is generally considered more expansive coverage than one that offers one or the other.

60. *See* Anderson, *supra* note 48, at 564–65; Hurtaud et al., *supra* note 53, at 93–95; Um, *supra* note 51. Cyber insurance is expansive but it is not all encompassing. In particular, cyber insurers insist on sizeable deductibles and exclude the direct costs associated with paying a "ransom" to unlock malware, the direct costs of reputation and data destruction.

61. *See* Talesh, *Data Breach*, *supra* note 55, at 12.

62. *See id*.

63. *Id.* at 12–14.

Cyber insurers engage in considerable risk and loss prevention on behalf of the organizations that purchase their insurance and absorb many of the functions of the organizations in terms of preventing risks. Risk prevention takes a series of forms, including conducting cyber health checks and audits that evaluate the kinds of cyber security practices that the organization is maintaining.[64] After the evaluation is made, a health score is provided and the insurer offers recommendations concerning the organization's security and privacy practices.[65] Insurers then "scan" hidden risks on public-facing infrastructures, provide a detailed view of a company's vulnerability status, and prioritize vulnerabilities.[66] The insurer or the third-party vendor test the effectiveness of existing firewalls and web and e-mail servers and try to mitigate vulnerabilities. Insurers that I spoke with framed these services as very valuable because they go well beyond what many existing organizations currently offer in terms of cybersecurity protections.

In addition to trying to prevent data breach events from occurring, insurers offer services that try to detect breaches before they occur. For example, insurers offer "shunning" analysis.[67] Shunning uses intelligence and security technology to isolate and literally shun communications to and from IP addresses currently being used by criminals.[68] Professionals in the cyber security community that I studied repeatedly described these services offered by insurers and their third-party vendors as helpful.[69]

Insurers also regulate the relationships that organizations enter into with subcontractors that corporations contract with to perform services. Organizations face legal risks when hiring subcontractors because organizations may be held legally liable for its subcontractor's

64. *See* NetDiligence, Cyber Risk Assessments (2016), https://netdiligence.com/wp-content/uploads/2016/05/NetDiligence_QuietAudit-Assessments_2016-1.pdf. The cyber health check and evaluation is quite comprehensive, in that it evaluates (1) current events; (2) security policy; (3) security organization; (4) asset classification and control; (5) personnel security; (6) physical and environmental security; (7) computer and network management; (8) system development and maintenance; (9) business continuity planning; (10) security compliance; (11) internet liability; and (12) privacy and regulatory compliance. *See id.*; *see also* Talesh, *Data Breach*, *supra* note 55 (manuscript at 21) (highlighting how cyber health checks operate).

65. *See* Talesh, *Data Breach*, *supra* note 55, at 13.

66. *See Cyber Insurance*, AIG, http://www.aig.com/business/insurance/cyber-insurance (last visited Aug. 11, 2016); *Security Services*, IBM, https://www-03.ibm.com/secutiry/services/cyber security-assessment/ (last visited Aug. 11, 2016); *see aslo* Talesh, *Data Breach*, *supra* note 55 (manuscript at 21).

67. *See Cyber Insurance*, *supra* note 66 (discussing how shunning works to prevent data breach events); Talesh, *Data Breach*, *supra* note 55, at 14.

68. *See Cyber Insurance*, *supra* note 66.

69. *See* Talesh, *Data Breach*, *supra* note 55, at 12–14.

data loss. To address this legal threat, the insurance field offers services that help measure and monitor the networks of vendors that an organization works with.[70] By providing this information to organizations considering which vendors to use, insurers allow organizations access into its vendor's security practices. This increases the likelihood that organizations will contract with cybersecure vendors and avoid legal liability. Thus, insurance companies are regulatory intermediaries because they help organizations identify subcontractors that are less likely to trigger a privacy law violation that will be imputed to the organization. In doing so, insurers help organizations properly interpret, implement, and comply with privacy laws.

Focusing on prevention and detection allows insurers to coach organizations on how to strengthen their cyber risk management program.[71] In doing so, the insurance company absorbs many of the functions of the information technology department and actively engages in loss prevention in a manner that organizations find quite efficient.

Consistent with scholars who are optimistic about the role of insurance-as-regulation, these risk prevention tools and security ratings play an important regulatory role over organizations. The scans and health checks are sometimes used as a precondition for determining whether a potential company is eligible for cyber insurance. Organizations interested in insurance protection, therefore, are often interested in becoming more cyber secure. Also, the more a company is cyber secure and has good preventative tools in place, the greater likelihood the insurance company will lower premiums.

1. *Insurer Risk-Management Services Strengthen Organizational Compliance Through Written Training Materials and Telephone Hotlines that They Offer*

Risk assessments and audits are not the only ways that insurers regulate the decision making and behavior of organizations. Insurers construct the meaning of compliance through a series of written value-added services that focus on advising organizations on how to prevent and detect data breaches. The written materials offered by insurers are quite comprehensive. Cyber insurers offer organizations hundreds of forms and documents, including access to cyber news and blogs,

---

70. *See id.* at 14 (discussing how insurers screen the cyber security practices of the prospective subcontractors and provide information to the organizations so that they can choose cyber secure partners).

71. *See id.* at 12–14. In fact, many panelists at conferences and many organization representatives that I talked with referred to cyber insurers as effective coaches.

best-practices checklists, monthly newsletters, articles and whitepapers, videos, and webinars, and legal summaries and updates, including some that address new and amended privacy laws.[72] These documents advise organizations on how to avoid fines and liability for data breach. Cyber insurers also evaluate an organization's written policies, procedures, forms and handbooks to determine if they comply with federal and state law. In particular, these written audits focus on interpreting privacy laws and preventing breaches that lead to regulatory fines.[73] Finally, organizations are provided access to an insurer-run website that includes resources on how to train staff, to identify exposure to loss, and to stay informed as compliance issues evolve.[74] In this respect, insurers are shaping the way that private organizations comply with privacy law challenges on the ground.

Insurers offer an incident response hotline made up of subject matter experts who know the latest vulnerabilities and cyber risk landscape and are able to provide specialized knowledge to clients to ensure that their cyber infrastructure is secure. Cyber insurer hotlines are focused not on offering legal advice (unlike EPLI insurer risk management services that I will discuss later in this article), but on heightening the security systems of companies and preventing any data loss.[75]

Taken collectively, these risk management services have potential positive impacts on compliance. No organization or consumer wants to have their data compromised. Insurance companies offering these services may reflect some best practices, prevent data theft breaches, and lead to improved compliance. To the extent it does, both consumers and organizations greatly benefit. Moreover, unlike in other settings such as employment practice liability insurance,[76] insurance

---

72. *Id*. at 9 fig. 1 (noting that legal interpretation of privacy laws as one of the components); *see, e.g.*, *CyberEdge End-to-End Cyber Risk Management Solutions*, AIG, http://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/aig-cyberedge0418finalsingle-brochure.pdf (last visited Aug. 12, 2016); *Services*, NetDiligence, http://netdiligence.com/services (last visited Aug. 9, 2016); *see also* Um, *supra* note 51.

73. *See* Talesh, *Data Breach*, *supra* note 55, at 15 (highlighting the wide variety of written services offered); *see also CyberEdge*, *supra* note 72; *Onsite Cyber Risk Assessment*, NetDiligence, http://netdiligence.com/portfolio/assessment/ (last visited Aug. 9, 2016).

74. *See* Talesh, *Data Breach*, *supra* note 55, at 9 fig. 1 (highlighting the wide variety of written services offered). *See generally CyberEdge*, *supra* note 72; *Onsite Cyber Risk Assessment*, *supra* note 73.

75. AIG, *Cyber Series, IBM Security*, YouTube (Sept. 3, 2015), https://www.youtube.com/watch?v=oq4cGHV2WJ0 (explaining that the hotline is "where subject matter experts may be reached instantly to discuss potential indicators of compromise to determine if, and how, a compromise may have occurred, with advice on what immediate steps to take to address vulnerabilities and contagion").

76. *See supra* note 14 and accompanying text.

company guidance on these issues does not largely focus on how to avoid litigation, but on how to prevent data theft losses in the first instance. Thus, the cyber insurance example provides empirical evidence for the claim that insurers act as risk regulators in ways that further compliance goals and foster heightened safety and security for the organizations and most importantly, its clients and customers.

2. Cyber Insurance Provides Risk Management Services that Help Organizations Respond in the Event of a Data Breach

The regulatory interventions of cyber insurers go beyond risk prevention and detection. Insurers influence the way that organizations respond in the event of an actual data breach. In addition to covering legal defense and indemnification costs associated with a covered loss, cyber insurers cover the legal, forensic investigation, business interruption, crisis management, and credit monitoring and restoration expenses. However, insurers do not just pay for the costs of these services, they also provide access to services aimed at responding to, investigating, defending, and mitigating against the consequences surrounding a data breach event or privacy law violation.[77] Insurers contract with third-party vendors that the insured can use or have departmental units that deal with various cyber-related problems.[78] Typically, the insured receives a reduced premium to use the insurer's vendors.[79] Cyber insurers are providing risk response well beyond the scope of what insurers typically handle.

Typically, corporations facing a cyber violation have incident response teams that manage and coordinate the data security event investigation, response, reporting and the corrective action taken. The incident response team often consists of: a team leader; a privacy officer; the departments of legal and risk management services, information security, human resources, employee relations, and patient relations; outside legal counsel (who is often the breach coach); a crisis management and public relations person; a forensics person; and an insurance company or its broker.[80] Corporations use and identify many of the team members from insurance company vendor lists that insurers provide to corporations.[81] Organizations found the access to

77. *See* Talesh, *Data Breach*, *supra* note 55, at 16–19 (highlighting the various value-added services that insurance companies offer); *see also* Anderson, *supra* note 48, at 603–07 (highlighting the various value-added services that insurance companies offer).

78. *See* Talesh, *Data Breach*, *supra* note 55, at 16.

79. *See id.* at 16.

80. *See id.* (discussing the key individuals involved in the incident response team).

81. *Id.*

these services and the "one-stop shopping" in the event of a data breach to be invaluable.[82]

Insurers help with providing organizations access to a designated panel of lawyers and law firms that can assist in managing the legal issues that arise when a data breach occurs.[83] These law firms help organizations prepare for and respond to data security incidents and assist with complying with various privacy laws and regulatory provisions largely focused on making sure consumers are notified in a timely manner that there is a data breach.[84] Legal advice is particularly useful because there are forty-seven state consumer notification statutes with various requirements.[85] Private organizations refer to these lawyers as their "breach coach," capable of guiding the organizations through the regulatory maze and making sure organizations respond in a way that does not trigger further problems.[86] In addition to offering twenty-four hour access via an 800 number, these lawyers play a critical role in developing and managing the incident response team that is formed when a data breach occurs.[87] Corporations appreciate being able to access a menu of law firms that have already been screened by the insurer.[88]

In addition to providing legal expertise, insurance institutions are the primary source of forensic expertise. Cyber insurers help organizations respond when a cyber security system is breached, identify the source and cause of the data breach, contain the breach, and ultimately restore the network processes that may have been damaged as a result of the breach.[89] Cyber insurers or their third-party vendors offer forensic cyber security experts to organizations. In my fieldwork, access to forensic experts was repeatedly seen as one of the

---

82. *Id.*

83. *Id.* at 17 (discussing how insurers offer organizations access to legal services through their network).

84. Um, *supra* note 51 ("[A]ttorneys assist with notification if a data breach occurs and to defend lawsuits following such notification.").

85. *Id.* ("47 states have consumer notification laws, and policyholders need the assistance of experienced attorneys to evaluate which state laws have been triggered and what steps policyholders must take following a data breach event.").

86. Talesh, *Data Breach*, *supra* note 55, at 17 (discussing the role of the breach coach); *see* Jeffrey D. Brunken, *Is Cyber Insurance a Good or Bad Investment?*, PHYSICIANS PRAC. (Nov. 24, 2013), http://www.physicianspractice.com/print/189788 (noting breach coach provides a main point of contact for the policyholder).

87. *See* Talesh, *Data Breach*, *supra* note 55, at 17 (noting the pivotal role the breach coach plays).

88. *Id.* at 16–18.

89. *Id.* at 17–18 (discussing the need for the forensic expert to come in and address the data security breach); Um, *supra*, note 51, at 1 (discussing the need to contain the source of the breach and restore the network processes).

most valuable services offered by cyber insurers.[90] Cyber insurers not only provide the insured access to these vendors, but they cover the costs to retain information security forensics experts, identify the source of the breach, contain the breach, and restore the network processes back to normal.[91]

Another major threat organizations face when a data breach occurs is severe or even terminal damage to its reputation.[92] Cyber insurance addresses this risk by covering the costs to retain the services of a public relations and crisis management firm.[93] However, cyber insurers go beyond providing coverage by offering a series of preapproved public relations and crisis management firms that the insured can retain at a reduced premium.[94] These crisis management and public relations firms develop and provide advertising or related communications to protect and restore the insured's reputation following a breach event.

Finally, cyber insurers provide access to companies experienced in credit monitoring and restoration that organizations can use for a reduced fee.[95] In addition, cyber insurance covers the costs of credit monitoring, fraud monitoring and setting up call centers to respond to customer concerns and inquiries as a result of data loss.[96] These value-added services are crucial because consumers are at risk of credit and identity theft by hackers when their financial information is stolen. Financial institutions, retail stores, and credit card companies that experience breaches of consumer information often set up credit monitoring and restoration services for consumers. This typically also includes establishing a call center to respond to customer concerns and inquiries regarding data breach events. When evaluating the totality of services that the insurers offer organizations, such as the legal

---

90. Talesh, *Data Breach*, *supra* note 55, at 17–18.

91. Anderson, *supra* note 48, at 604 ("Cyber risk policies often provide coverage for the investigatory costs associated with determining the cause and scope of a breach or attack.").

92. *A Data Breach Isn't Always a Disaster. Mishandling It Is.*, BEAZLEY, https://www.beazley.com/specialty_lines/data_breach.html (last visited Aug. 9, 2016). In particular, studies show that a third of customers of companies that suffer a data breach refuse to continue doing business with that company in the future. *Id.*

93. Anderson, *supra* note 48, at 604–05 ("[T]he costs associated with a cyber attack often include crisis management activities.").

94. Talesh, *Data Breach*, *supra* note 55, at 18 (noting that in addition to covering the costs relating to crisis management, insurers offer policyholders access to firms that specialize in crisis management).

95. *Id.* (noting that cyber insurers offer access to organizations that handle credit monitoring and restoration in addition to paying the costs of such services).

96. Anderson, *supra* note 48, at 603 ("Cyber risk policies typically provide coverage for the costs associated with notification of a data breach and credit monitoring services.").

services, forensics, public relations, and crisis management, the insurer can be seen as the manager and regulator of cyber security risks.

Amidst an environment where organizations are *under-complying* with privacy laws and *under-prepared* for potential data breach events, cyber insurers are intervening and acting as regulatory intermediaries. Cyber insurers are doing much more than pooling and spreading risk. The incident response team for organizations dealing with privacy laws and cyber breaches is heavily influenced by insurers. In addition to providing defense and indemnification for losses resulting from data breaches, insurers are involved in the legal, forensic, information technology, credit monitoring, and public relations decisions relating to a data breach event. Insurers either offer an insured its risk management services or access to its network of third-party vendors who specialize in dealing with these various issues. By offering a series of risk management services developed within the insurance field that are aimed at preventing, detecting, and responding to cyber security breaches, insurance institutions actively shape the way an organization responds to data theft. Consistent with Logue and Ben-Shahar's concept of insurance as risk regulation, insurers are acting as regulators in a way that better protects consumers and organizations. In this respect, the cyber insurance example is consistent with insurance law scholars' argument that insurance risk management can improve compliance and reduce moral hazard behavior of organizations. However, I extend the analysis by highlighting the specific risk management techniques insurers use to curb data breach events from occurring.

B. Insurance Risk Management in the Corporate Securities Law Context: The Bad

Despite the obvious financial incentives insurers have for getting involved in the cyber security risk management market, the cyber insurance example highlights how insurer risk management services can help curb the under-compliance and under-preparation gaps that organizations encounter when dealing with cyber threats. In particular, insurance company interventions aimed at preventing, detecting and responding to cyber threats simultaneously help the regulated entities (organizations who do not want to experience a data breach) but also help consumers (who do not want their private information compromised). Although not perfect, insurance institutions help corporations protect client and customer data and behave in a more socially responsible manner.

Insurance companies do not, however, always have positive outcomes as corporate regulators. Insurance companies offering directors' and officers' liability insurance highlight how insurance companies are not always effective substitutes as regulators. If insurance companies as corporate regulators dealing with privacy and cybersecurity issues are largely positive, here, insurance company behavior as corporate regulators of directors and officers are largely negative.

In particular, direct litigation by shareholders is an important regulatory mechanism over U.S. corporations. Given the limits of public regulation, a variety of legal tools are left in the hands of shareholders. Shareholders that believe they have been wronged by the corporation that they have invested in can sue as a class or on behalf of the company itself to seek relief. This litigation is often referred to as "shareholder litigation."[97] Broadly, shareholder litigation refers to all civil actions brought by current or former shareholders of a corporation against the corporation or its managers for losses the shareholders suffer as a result of actions taken by the corporation and its managers.[98] Acting as a private attorney general, shareholders have strong personal incentives to detect and prosecute corporate wrongdoing.[99] Such litigation is supposed to deter corporate misconduct and serve as a regulatory check on directors and officers tasked with managing and running the corporation.[100]

In response to the very real threat of shareholder litigation, officers and directors of corporate entities often obtain Directors' and Officers' Liability Insurance (D&O insurance). This insurance protects officers and directors from personal liability in the event of shareholder litigation.[101] Moreover, D&O insurance also protects the corporation itself from liability it may have in connection with shareholder litigation. D&O insurance transfers the obligations of the prospective bad actor (officer, director, or corporation itself) to an

97. *See, e.g.*, TOM BAKER & SEAN J. GRIFFITH, ENSURING CORPORATE MISCONDUCT: HOW LIABILITY INSURANCE UNDERMINES SHAREHOLDER LITIGATION 3–5 (2010) (explaining shareholder litigation); Robert B. Thompson & Randall S. Thomas, *The New Look of Shareholder Litigation: Acquisition-Oriented Class Actions*, 57 VAND. L. REV. 133, 135–36 (2004); *see also* Jill E. Fisch, *Confronting the Circularity Problem in Private Securities Litigation*, 2009 WIS. L. REV. 333, 339 n.24, 340 n.27 (2009); Paul Weitzel, *The End of Shareholder Litigation? Allowing Shareholders to Customize Enforcement Through Arbitration Provisions in Charters and Bylaws*, 2013 B.Y.U. L. REV. 65, 67 (2013).

98. BAKER & GRIFFITH, *supra* note 97, at 3.

99. *Id.* at 1 (noting that public regulators cannot oversee every company and thus shareholders have "strong personal incentives to detect and prosecute corporate wrongdoing").

100. *Id.* at 1–2. The deterrence impact here is that prospective wrongdoers realize that they may be sued for any harms that they cause and thus have a strong incentive to not engage in corporate misconduct. *Id.*

101. For a thorough explanation of directors' and officers' insurance, see *id.* at 10–13.

insurer which pays for defense and indemnification.[102] Thus, one concern is that D&O insurance potentially decreases the deterrence function of shareholder litigation by making it easier for directors and officers to pass these risks and responsibilities to the insurance company.[103]

By offering D&O insurance, however, insurers act as a third-party intermediary in the regulatory scheme. In this situation, directors' and officers' insurers have a great opportunity to influence corporate conduct through the insurance relationship to potentially help directors and officers avoid shareholder litigation.[104] After all, if insurers are ultimately going to have to pay for the harms caused by their corporate insureds, insurers have ample incentive to exert a regulatory influence over the directors and officers, and have the opportunity to do so. D&O underwriters conduct a thorough examination of the governance features of prospective insureds, evaluate risk factors and structural governance features. D&O insurers have opportunities to influence corporate conduct through underwriting, monitoring and the settlement of claims. In theory, this provides a basis for loss-prevention guidance. Successful oversight of directors and officer behavior and conduct would preserve shareholder litigation as a regulatory device and encourage corporate actors to engage in compliant behavior.

However, empirical research suggests that although D&O insurers have an opportunity to influence the behavior of directors and officers and discourage wrongful and even illegal behavior by acting as regula-

---

102. *Id.* at 10–11. To the extent that insurance hinders or weakens deterrence, it undermines the basic justification for shareholder litigation. *Id.*

103. *Id.* at 11 ("This creates a problem for deterrence. With liability risk transferred to a third-party insurer, prospective defendants are no longer forced to internalize the full cost of their actions. With little or nothing at risk, in other words, they are unlikely to be deterred from the sorts of actions that may lead to shareholder litigation.").

104. Baker and Griffith note the powerful ways that D&O insurers could regulate director and officer behavior:

> D&O insurance has the potential to insulate corporations and their managers from the consequences of liability rules that are expressly designed to penalize bad governance and encourage good governance. As a result, the D&O insurer thus assumes a pivotal role in the analysis. The question thus becomes, Does the D&O insurer have some means of passing along the deterrent effect of shareholder litigation or does the fact of D&O coverage distort or destroy the accountability mechanisms build into shareholder litigation? In other words, what do D&O insurers do to deter bad acts on the part of their insureds? Since, after all, the insurers are the ones ultimately footing the bill for shareholder claims, they would seem to have ample incentive to control the conduct that might lead to claims.

BAKER & GRIFFITH, *supra* note 97, at 13.

tory intermediaries, they rarely do so.[105] Tom Baker and Sean Griffith's empirical study of the relationship between directors' and officers' insurance and corporate actors reveals that D&O insurance significantly weakens the deterrent effect of shareholder litigation and thus undermines such private attorney general suits as forms of regulation.[106]

Despite having financial incentives to do so, D&O insurers neither monitor nor provide loss prevention programs to the corporations they insure.[107] In particular, D&O insurers do not condition the sale of insurance on adopting loss-prevention policies.[108] Moreover, brokers and risk managers note that loss prevention advice was not very valued or binding on public corporations.[109] With only one exception, Baker and Griffith's research revealed that none of the underwriters or brokers they interviewed could recall a single situation in which a publicly traded corporation changed a business practice in response to a governance concern raised by a D&O insurer.[110]

Equally important, insurers rarely try to influence or change corporate behavior.[111] While insurers servicing private corporations routinely provide corporations access to newsletters, conferences, and written materials relating to good governance, insurers do not condition insurance coverage on adopting any governance practice, providing loss-prevention audits, or even providing clear discounts for adopting what insurers might consider good corporate governance standards.[112] Insurers often resist offering loss prevention advice, in part, because they cannot empirically show that adopting insurer recommendations leads to reduced loss.[113] Baker and Griffith note that one insurer who tried to encourage corporations adopt their loss pre-

105. *Id.* at 126–27 (highlights how insurers fail to engage in loss prevention with directors and officers).

106. *Id.* at 103–04, 126–27 (examining how insurers fail to sufficiently deter misconduct through pricing and underwriting, monitoring, loss prevention, and settlement practices).

107. *Id.* at 126–27 (finding that insurers have opportunities to engage in loss prevention but fail to do so).

108. *Id.* at 109 (finding that "D&O insurers do not condition the sale of insurance on compliance with loss-prevention requirements in any systematic way").

109. *Id.* ("Although D&O insurers do occasionally provide loss-prevention advice, underwriters report—and brokers and risk managers confirm—that this advice is not highly valued by public corporations, nor is it in any way binding on corporations as, for example, a condition of policy renewal.").

110. BAKER & GRIFFITH, *supra* note 97, at 109.

111. *Id.* at 109–10 ("Our participants were nearly unanimous in reporting that insurers are not successful at getting public companies to change their governance practices, and indeed that they rarely ever try.").

112. *Id.* at 111.

113. *Id.* at 112–13.

vention programs ultimately abandoned such an approach: "[W]ithout a bundled premium discount, companies were unwilling to follow the insurer's loss-prevention program, especially when competing insurers were offering the same insurance without any loss-prevention requirements."[114]

D&O insurance brokers also do not step in and engage in harm or loss prevention despite opportunities to do so. Unlike the cyber insurance context where insurers actively engage in loss prevention, brokers do not offer advice about what governance programs are likely to count negatively when the insurer conducts an underwriting assessment.[115] Brokers identify features of the corporation that are likely to be evaluated positively by insurers;[116] however, insurers do not make attempts to nudge the corporation in a more compliant direction.[117] Although brokers negotiate with insurers to structure the various layers of insurance and use market power to pressure insurers to settle when claims are made, they do not monitor corporate insureds.

What does all this mean for corporate executives that are the target of shareholder litigation? It means that corporate executives purchase D&O insurance with shareholder money and essentially shift the vast majority of malfeasance and misconduct risks away from themselves while operating at a publicly traded company. Insurers offer little advice or risk management and top executives ask for little assistance in monitoring or managing the day-to-day operations. Thus, corporate officers are able to gain the benefits of insurance coverage and protection without yielding any control over the day-to-day operation of the corporation. Corporate executives are able to purchase and gain these benefits at the expense of the shareholders.[118]

Directors' and officers' insurers not only fail to play a role in the monitoring and oversight of corporate executives, but also fail to exert control over defense and settlement. In theory, insurers could manage defense and settlement of shareholder claims, fight frivolous

114. *Id.*

115. *Id.* at 113–14. Baker and Griffith noted that "advice about how to avoid a negative underwriting assessment and put one's best foot forward in the market for insurance is relatively piecemeal—a far cry from a comprehensive program about how to implement structures that will avoid D&O losses. Brokers principally offer marketing advice." *Id.* at 113.

116. BAKER & GRIFFITH, *supra* note 97, at 113–14.

117. *Id.* at 116 ("The broker helps the prospective insured put its best foot forward in purchasing insurance, but the broker does not counsel his or her client on how to modify its corporate governance structure.").

118. As Baker and Griffith note, "Top executives in public corporations are thus able to purchase income-smoothing insurance without ceding any governance authority to insurers because this purchase, like all such decisions, is insulated from shareholder challenge by the business-judgment rule." *Id.* at 127.

claims, manage defense costs, and withhold insurance benefits from directors and officers who have engaged in actual fraud. Specifically, insurers could make sure that cases are resolved on the merits and that settlement amounts bear a close relationship to the harm caused by the director so the insurance loss costs used in the D&O insurance pricing formulas provide the right signal. Moreover, insurers could force defendants in the worst cases of egregious misconduct to pay more toward the defense and settlement of their claims. This would incentivize corporate insureds to avoid the kinds of misconduct that leads to a reduction in coverage. However, empirical research in this area suggests that insurers do very little to effectively manage defense and settlement. Although D&O insurers sometimes use their settlement control to extract concessions from corporate defendants, the settlement process often prevents D&O insurers from requiring that final settlement amounts track the underlying merit of claims.[119] Although insurers have some control over settlements, they have very little control over the conduct of the defense.[120] Baker and Griffith note, "Our criticisms of the process revolve principally around the lack of transparency of D&O insurance program structure and pricing as well as the precise contribution of D&O insurers to class action settlements."[121]

In sum, insurance companies are doing a very poor job of acting as corporate regulators in the directors and officers context. Even though D&O insurers are in a position regulate the behavior of directors and officers, they do very little to monitor and control the conduct of their corporate insureds. In theory, loss prevention should be a routine part of the package of services that any insurer provides. After all, insurers have the right incentives, the means to hire the proper experts, and shareholders and officers should highly value this service. Although loss prevention and risk management programs are common in other areas of insurance, they are typically not offered by D&O insurers in a meaningful way. Moreover, when loss prevention advice is provided, it is communicated as a suggestion rather than as a

119. *Id.* at 174–75. In particular, factors that influence settlement values include "(1) investor loss, (2) insurance limits and structure, (3) sex appeal, (4) litigation dynamics, and (5) statistical information from other settlements. Although some of these features clearly have merits–relevant aspects, notably investor loss and sex appeal, others, such as insurance limits and structure and litigation dynamics, clearly do not, and we tend to doubt that settlement statistics as used today push in the merits-relevant direction." *Id.* at 176.

120. *See id.* at 128–51. In particular, "D&O insurance policies give insurers no direct control over the conduct of the defense and how, in fact, D&O insurers have little ability to control defense costs. Their authority over settlements is significantly constrained by the threat of being found to have acted in bad faith by unreasonably withholding consent to settle." *Id.* at 150–51.

121. *Id.* at 176.

mandate and is designed more to promote or market the insurer than to restrict the conduct of the insured. While capable of engaging in corporate oversight and regulation, insurers simply sell this insurance at a profit to a population eager to purchase such insurance. D&O insurers play little to no role in regulatory oversight.[122] Moreover, the impact of shareholder litigation on directors and officers can now be more easily passed off to insurers without causing the corporate officers much discomfort. Thus, similar to the cyber security context, the interests of the consumer and corporation are aligned, but in this instance insurers fail as regulators. The D&O insurance example highlights an example of how insurer risk management does not induce positive regulatory outcomes.

C. Insurance Risk Management in the Employment and Anti-Discrimination Law Context: The Ugly

If insurance company regulator interventions are relatively helpful concerning corporations dealing with privacy laws and cyber security threats, and unhelpful in preventing corporate misconduct, then insurer regulatory interventions in the employment law context can be described as at best, ugly. I use the term "ugly" because whereas D&O insurers had opportunities to engage in loss prevention and discourage wrongful or even illegal conduct but failed to do so, employment practice liability insurers do offer risk management and loss prevention advice but do so in a way that often weakens the meaning of anti-discrimination law and reframes anti-discrimination law around a focus on risk and litigation avoidance.

The rise of Employment Practice Liability Insurance (EPLI) illustrates how insurance institutions mediate the meaning of compliance with civil rights legislation and how these constructions of compliance end up being deferred to and legitimated by public legal institutions. Prior to the development of employment discrimination law, workers suffering workplace discrimination or harassment seldom sought or brought lawsuits.[123] Title VII and other civil rights laws try to convert the guarantees established by the U.S. Constitution into legislation

122. I do not mean to suggest that it is very easy for insurers to act as regulators. In the corporate securities context, a series of institutional barriers prevent D&O insurers from bundling loss-prevention programs with D&O insurance, including 1) a lack of underwriter knowledge and experience; 2) characteristics of securities misinformation losses that may make monitoring futile or prohibitively costly; 3) the layered, excess-of-loss structure of D&O insurance programs; and 4) the insurance underwriting cycle. BAKER & GRIFFITH, *supra* note 97, at 118–24.

123. Joan Gabel et al., *Evolving Conflict Between Standards for Employment Discrimination Liability and the Delegation of That Liability: Does Employment Practices Liability Insurance*

that addresses specific issues such as workplace discrimination and harassment.[124]

In response to perceived threats of employment discrimination lawsuits, insurance companies began offering EPLI. Unlike prior forms of business insurance that expressly excludes coverage for liability arising out of employment practices, EPLI provides employers with the ability to manage the increasing litigation risk associated with discrimination, sexual harassment, wrongful termination, and other breaches of employment law.[125] EPLI policies provide insurance defense and indemnification coverage to employers for claims of discrimination (e.g., age, sex, race, disability) and other employment-related allegations made by employees, former employees, or potential employees.[126]

Insurers increasingly offer EPLI and employers increasingly purchase this insurance. Whereas only a few insurance companies in the 1990s offered EPLI, now over seventy insurance companies offer EPLI and many large employers purchase EPLI.[127] Insurers play a role in averting such risk and act as a regulatory intermediary because employers have an incentive to avoid discrimination; however, insurers do so in a way that focuses on avoiding litigation rather than fostering a discrimination-free work environment.

Specifically, my fieldwork revealed how the insurance field (insurance companies, agents, brokers, and risk management consultants), through EPLI and the accompanying risk management services that

---

Offer Appropriate Risk Transference?, 4 U. PA. J. LAB. & EMP. L. 1, 5 (2001) (noting that litigating over discrimination is a relatively recent phenomenon).

124. Title VII in particular states in relevant part:

> It shall be an unlawful employment practice for an employer—
>
> (1) to fail or refuse to hire or to discharge any individual, or otherwise to discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual's race, color, religion, sex or national origin . . . .

Civil Rights Act of 1964 § 703, 42 U.S.C. § 2000e-2(a)(1) (2012); *see also* Civil Rights Act of 1991, Pub. L. No. 102-166, 105 Stat. 1071 (codified as amended at 42 U.S.C. § 2000e (2012)) (emphasizing the deterrent effect of financial liability by providing compensatory and punitive damages for disparate treatment lawsuits brought by private plaintiffs). *See generally* U.S. CONST. amend. XIV, § 1.

125. *See* Joan T.A. Gabel et al., *The Peculiar Moral Hazard of Employment Practices Liability Insurance: Realignment of the Incentive to Transfer Risk with the Incentive to Prevent Discrimination*, 20 NOTRE DAME J.L. ETHICS & PUB. POL'Y 639, 640, 650–51 (2006) (highlighting the rise of EPLI); *see also* Gabel et al., *Evolving Conflict*, *supra* note 123, at 28–30.

126. *See* Nancy H. Van der Veer, Note, *Employment Practices Liability Insurance: Are EPLI Policies a License to Discriminate? Or Are They a Necessary Reality Check for Employers?*, 12 CONN. INS. L.J. 173, 175–77 (2005) (explaining what is EPLI is and the range of coverage).

127. *See* Talesh, *A New Institutional Theory of Insurance*, *supra* note 5, at 626 (noting the increase in the number of insurers and employers that offer and purchase this insurance).

the field offers, construct the threat of employment law and influence the nature of civil rights compliance.[128] Drawing from participant observation and interviews at EPLI conferences across the country as well as content analysis of EPLI policies, loss-prevention manuals, EPLI industry guidelines, and webinars, my empirical data suggest that insurance companies and institutions use a risk-based logic and institutionalize a way of thinking centered on risk management and reduction.[129] Faced with uncertain and unpredictable legal risk concerning potential discrimination violations, insurance institutions elevate the risk and threat in the legal environment and offer a series of risk-management services that they argue will avert risk for employers that purchase EPLI.[130] By framing employers' legal environment in terms of uncertain legal risk,[131] heightened litigation risk,[132] and the need for risk reduction,[133] the insurance industry creates a space to encourage employers to engage in managerialized responses and develop formalized policies and procedures by using the various risk-management services offered by insurers to help reduce these risks.

My empirical research in this area went beyond analyzing the uncertain legal risks employers face and the high likelihood that employers are going to be sued. My fieldwork revealed that insurers encourage employers to purchase EPLI because these insurance policies and the value-added risk management services that insurers offer will reduce employers' risk.[134] In particular, EPLI insurers offer a va-

128. For a thorough explanation of how insurers focus their guidance on avoiding litigation rather than a discrimination-free work environment, see *id.* at 626–32; Talesh, *Legal Intermediaries*, *supra* note 6, at 209–34.

129. *See* Talesh, *Legal Intermediaries*, *supra* note 6, at 219–21.

130. *Id.* at 219–23 tbls.1, 2, 3 & 4 (highlighting a series of examples of how insurers frame legal risk as uncertain, heighten litigation risk, and encourage reducing risk).

131. Uncertain legal risk refers to the risk of loss to an organization based on some violation of law. My empirical research reveals that insurers frame employers' legal risk as uncertain, vague, and unpredictable. *See id*. at 218–19 for comprehensive analysis of how the insurer field frames employers' legal risk as uncertain.

132. Insurance field actors heighten the litigation risk facing employers by routinely discussing the growth, burden, and cost of employment lawsuits in documentary data and webinars: "Not-for-profit corporations and public entities, in addition to public and private businesses, are experiencing an explosion of employment-related claims." GARY W. GRIFFIN ET AL., THE EPL BOOK: THE PRACTICAL GUIDE TO EMPLOYMENT PRACTICES LIABILITY AND INSURANCE 1 (3d ed. 2001). For further analysis of how the insurer field heightens employers' litigation risk, see Talesh, *Legal Intermediaries*, *supra* note 6, at 219–21.

133. Talesh, *Legal Intermediaries*, *supra* note 6, at 221 ("Once the insurance field frames the legal risks facing employers as uncertain but elevated and likely to occur, the insurance field encourages employers and risk management consultants to avert or reduce this risk by purchasing EPLI insurance and the accompanying risk-management services."). For further analysis of how the insurer field encourages employers to reduce and avert risk by purchasing EPLI, see *id.* at 221–23.

134. *Id.* at 223–31.

riety of risk-management services to employers that try to provide a regulatory check on employer discriminatory practices. ELPI insurers conduct compliance audits of employers and offer employers a confidential legal hotline that allows employers to ask legal questions to insurer-sponsored lawyers.[135] They also provide employee handbooks and employment "contract builders" to employers so that they can construct a handbook and develop contracts without actually drafting the documents.[136]

Insurer risk-management services can have positive and negative impacts on compliance. On the one hand, insurer risk management practices may reflect some best practices and lead to improved employment policies and procedures. On the other hand, they may also make it easier for employers to develop policies and procedures without actively participating in the creation of these policies and procedures. In particular, insurance company guidance on these issues largely focuses on how to avoid litigation as opposed to focusing on EPLI insurers' often-stated goal of providing mechanisms for building a discrimination-free work environment.[137]

Whereas insurers in the privacy context focus less on interpreting or influencing the meaning of privacy law, EPLI insurers influence the *meaning* of compliance with anti-discrimination laws in a number of ways. First, conferences, training programs, loss-prevention manuals, and insurance policy language provide an opportunity for the insurance field actors to build discretion into legal rules.[138] In other words, insurance companies develop policy language, which provides work-arounds to certain legal rules clearly forbidding insurance coverage for certain acts or omissions in civil rights contexts.

For example, the insurability of punitive damages highlights how the insurance field builds discretion into legal rules. Even though civil rights laws can potentially subject employers to punitive damages and many states prohibit the insurability of such damages,[139] EPLI insurers build discretion into their policies and broaden coverage to include

135. *Id.* at 229 (discussing risk-management programs insurers offer, including telephone hotlines, audits, and a series of written materials that employers can use to create, develop, or enhance their own employment practice materials).

136. *Id.* at 230–31.

137. *Id.* at 222–25.

138. *See id.* at 225–26.

139. *See* RICHARD S. BETTERLEY, BETTERLEY RISK CONSULTANTS, INC., EMPLOYMENT PRACTICES LIABILITY INSURANCE MARKET SURVEY 2012: RATES CONTINUE TO FIRM, BUT NOT FOR ALL CARRIERS 9 (2012) ("We understand that there are 16 states that prohibit or restrict coverage for either Punitive Damages and/or Intentional Acts . . . ."), http://betterley.com/samples/EPLI12_nt.pdf.

punitive damages by including "most favored venue" clauses into their policies.[140] In particular, these clauses indicate that the enforceability of insurance coverage shall be governed by the applicable law that most favors coverage for punitive and exemplary damages. Not surprisingly, insurance companies list state jurisdictions in their policies, which the insurance companies must consult in determining insurability, that often permit coverage for punitive damages.[141] Thus, even though statutes and caselaw often prohibit coverage for punitive damages, these damages are covered by EPLI. Under the framework of risk management and risk aversion, EPLI limits the ability of state and federal civil rights laws to hold employers directly responsible for paying punitive damages because employers now have the ability to transfer these costs to insurers. Unlike the D&O context where insurers fail to step into the regulatory void concerning corporate malfeasance, EPLI insurers are stepping in and providing services in a manner that makes the regulatory impact of certain anti-discrimination laws harder to achieve.

Insurance companies also reframe legal rules and principles around a nonlegal risk logic that focuses on averting risk and making discrimination claims against employers more defensible. For example, insurers spend considerable time at conferences and training sessions discussing workplace bullying—a relatively new workplace issue that is now being increasingly litigated by plaintiffs' lawyers.[142] Although insurance institutions have an opportunity to encourage more lawful conduct in light of changing anti-discrimination laws, insurance field actors shift responsibility for fostering a safe and positive workplace away from employers. They do so by communicating how EPLI provides coverage for employers in the event that an employee is found liable for bullying: "Don't worry. EPLI has a catch all for these situations. Bullying claims fall within the definition of wrongful act in the policy—it is a wrongful workplace policy or procedure."[143] Thus, whereas insurers in the cyber security context coach organizations on how to prevent a data breach from occurring, here insurers are simply transferring risk without providing preventative guidance.

---

140. For a thorough examination of how employment practice liability insurers develop ways to provide coverage for punitive damages against its insureds, see Talesh, *Legal Intermediaries*, *supra* note 6, at 223–25.

141. *Id.* at 224. In addition, many insurers have offshore facilities in Bermuda and London or enter into relationships with foreign insurance companies to provide "wrap around" policies that will ultimately pay employers' punitive damages liability. *Id.* at 225.

142. *Id.* at 228.

143. *Id.* at 227–28.

Another example of how insurers reframe legal rules around concerns over risk is through Performance Improvement Plans (PIPs). Employment progressive discipline policies, such as PIPs, are often used as mechanisms to improve employee performance. PIPs are now framed by insurance field actors around managing risk and avoiding a negative inference from a jury at trial.[144] Specifically, while employers' normal practice is to provide PIPs prior to terminating employees, the insurance field routinely discourages using PIPs against employees who might be terminated.[145] Experts at conferences spend considerable time discussing whether insurance coverage exists for emerging forms of liability against employers as opposed to focusing on ways for employers to avoid committing legal violations in the first instance.[146] Thus, although the interventions that insurers provide in these settings is celebrated as providing a level of regulatory oversight, the reality is that the insurance field's message is focused on risk reduction.

Even U.S. Supreme Court decisions are framed by insurance field actors at conferences that insurers and employers attend around shifting risk and avoiding liability. When Supreme Court cases concerning employment law are discussed at EPLI conferences, EPLI risk-management consultants and lawyers steer employers toward avoiding liability and defending cases.[147] Thus, unlike the directors and officer context where insurers miss opportunities to engage in insurance loss prevention, insurers do engage in loss prevention, but do so in a manner that is filtered by risk-management logics. Law is viewed and understood as risk. While my data suggest EPLI and the series of risk-management services offered with the insurance policy can potentially

144. *Id.* at 226–27.

145. *Id.* at 226 ("PIPs are bad for litigation, 80 percent of people who receive a PIP end up being fired. Jurors view PIPs as a way to set someone up to be fired, especially if the employee raised a complaint or concern earlier.").

146. Talesh, *Legal Intermediaries*, *supra* note 6, at 226–27.

147. *See* Talesh, *A New Institutional Theory*, *supra* note 5, at 630–31. The Supreme Court case *Vance v. Ball State* curtailed the scope of who constitutes a supervisor in sexual harassment cases is illustrative. *See generally* Vance v. Ball State Univ., 133 S. Ct. 2434 (2013). In *Vance*, the Court established that a supervisor is one who has the ability to take tangible employment actions against the victim, such as hiring, firing, disciplining, promoting, and reassigning an employee. *Id.* at 2439–46.

> Rather than focusing on the proper role of supervisors, EPLI risk-management consultants and lawyers steer employers toward avoiding liability and defend cases. Risk-management consultants and attorneys suggest that employers not have many supervisors, selectively use the term "supervisor," clearly communicate levels of authority, and avoid behavior that gives an inference that the employee is a supervisor.

Talesh, *A New Institutional Theory*, *supra* note 5, at 630. "Field actors also dissuade employers from having lots of employees participate in training programs that could suggest an employee is a supervisor. Moreover, employers are encouraged to bring more motions for summary judgment since the law has narrowed the definition of supervisor." *Id.*

improve employment practices and compliance, they also suggest that EPLI risk-management services may at times shape compliance in a way that leans more toward making claims defensible rather than fostering a discrimination-free workplace.[148]

Despite the questionable regulatory outputs of insurers as risk managers in the employment context, my research reveals considerable deference to EPLI by public legal institutions, such as courts, legislatures, and regulatory institutions. In particular, federal, state, and municipal governments adopt risk logics of EPLI insurers and encourage, and at times require, public organizations and governmental institutions to purchase EPLI.[149] County and city state governments also increasingly rely upon EPLI and nudge other public entities to obtain such insurance.[150] Moreover, public secondary schools and public universities often require purchase of EPLI.[151]

As EPLI becomes an institutionalized service offered by insurers and purchased by public and private organizations, courts follow suit by significantly expanding the coverage afforded insureds under EPLI when interpreting coverage questions.[152] The expansive interpretation of EPLI by courts adds legitimacy to EPLI by authorizing, requiring, or encouraging public institutions to purchase such insurance and use the risk-management services that insurers offer.

Thus, the content and meaning of law and regulatory policy in this instance is determined by private organizations, such as insurance

148. In particular, "[r]isk-management and loss-prevention services allow insurers to not just shift risk off employers, but also to provide an opportunity for insurers to encourage managerialized responses and a formalization of policies and procedures in workplace settings." Talesh, *A New Institutional Theory*, *supra* note 5, at 631.

149. For a comprehensive analysis of the wide variety of public legal institutions including the Department of Justice, state governments, and public schools that defer to and encourage organizations to purchase EPLI, see *id.* at 631–35.

> In 1997, the U.S. Department of Justice Executive Office for U.S. Trustees approved EPLI insurance as an 'actual, necessary expense' of the trustee pursuant to her duties as trustee. This was based on the perceived increased number of lawsuits being filed concerning employment practices and the need for trustees to avert and reduce risk to themselves.

Id. at 631.

150. *Id.* at 632–33.

151. For a comprehensive analysis of the deference that schools give to EPLI, see *id.* at 633–34.

152. *Id.* at 633 n.83. In particular, courts have (1) "broadened the duty to defend by allowing for an unlimited right to insure under the duty to defend for intentional discrimination, even where the duty to indemnify has been limited"; (2) "expanded defense coverage of potentially nonindemnifiable acts, where it is unclear if such acts are nonindemnifiable at the pleading stage," (3) "held that there is indemnification coverage for disparate impact claims where any discrimination was unintentional," and (4) "redefined the intentional acts exclusion to require not just an intentional act but also deliberate wrongdoing." *Id.* at 633–34 n.83.

companies. The insurance field maintains a conception of employment law filtered through managerial and risk values, which highlights the enhancement of employers' formal structures that demonstrate compliance and rational governance. The insurance industry communicates and markets this vision by highlighting the risk of not developing policies and procedures, as well as by providing a protective net for employers in the form of D&O insurance coverage. The government adopts this conception into its policies by encouraging, authorizing, and sometimes requiring governmental institutions to purchase EPLI and the accompanying risk management services. Thus, legal mandates requiring organizations to purchase EPLI look like they emanate from public legal institutions, such as courts, legislatures, and regulatory institutions, but in reality the mandates are generated from the insurance field's responses to employment laws.[153]

The "ugliness" of insurance companies as regulators in the employment context lies in the manner in which insurers engage as regulatory intermediaries. In particular, EPL insurers translate and interpret the meaning of compliance in ways that build discretion into legal rules and recontextualize legal rules around a nonlegal risk logic that emphasizes averting risk and making discrimination claims more defensible. Risk and managerial values work together in the context of drafting, marketing, and selling EPLI. To the extent EPLI and the value-added services induce compliant behavior by private and public institutions, requiring organizations to purchase EPLI may lead to greater adherence to the civil rights goal of workplace equality. However, my empirical data suggest that at times there is a considerable disconnect between the moral values and rhetoric that legislators, judges, and lawyers use to discuss anti-discrimination law and the risk values and rhetoric that insurers use to suggest that litigation is inevitable and must be managed. Thus, it is surprising that courts and legislatures have deferred to, and at times encouraged, EPLI in some cases. The meaning of compliance with civil rights laws is at least partially constructed by the insurance field.

IV. Conclusion

In a world where corporations face increasing pressure to be responsible to not just shareholders, but its employees, customers, and the environment, corporations are turning to intermediaries, such as insurance companies, to assist with complying with the vast array of laws and regulations. This Article brings the role of insurance and

153. *See id*. at 625–35.

insurance institutions into a more direct conversation with concepts of corporate social responsibility and organizational responses to legal regulation. While prior research explores the role that intermediaries play in furthering corporate social responsibility and dealing with the various laws that impact organizations, there has been little focus on the role of insurance. Conversely, while prior insurance law scholarship celebrates the role of insurance companies as regulators, it largely focuses on how policy provisions, actuarial practices, and contracting allow insurers to act as risk regulators. However, there has not been as much empirical evaluation of how insurance companies tangibly act as risk regulators.

This Article suggests that insurers as risk regulators is not as positive as previously articulated by scholars. My conclusions are based on studies that unpack *how* insurer risk management techniques regulate organizational behavior on the ground. In the cyber security and privacy law context, insurer risk management services and interventions appear to be helping organizations avoid data breaches and violations with privacy laws. Insurers have intervened in a market where corporations admit to being under-prepared for data breach events, being under-compliant with privacy laws, and feeling a sense of "compliance fatigue."[154] Insurer risk management services are aimed at preventing, detecting, and responding to data breach events in ways that protect organizations and end-user consumers. Insurers focus less on communicating what the law means and more on how to stop data breach events. To that end, insurers are providing a high level of technical expertise aimed at combating evolving attempts to hack organizations' information. Insurers are acting as compliance managers and absorbing many of the functions that organizations feel they are unable to deal with. Insurers as risk managers appear to work well in the cyber insurance context, in part, because organizations and consumer interests are aligned in wanting to prevent any loss of personal information.

Of course, in the context of directors and officers, insurers do very little regulating even through insurers offer D&O insurance and have the opportunity to engage in loss prevention or monitoring. Insurers in this context are to some extent ensuring corporate misconduct and undermining the power of shareholder litigation because directors and officers can pass the costs of these lawsuits off to insurers. Thus, insurance in this context may increase moral hazard, or weaken the ability of law to nudge corporations toward more responsible behavior.

154. Armerding, *supra* note 50.

Insurers are unable and unwilling to act as risk regulators in the corporate governance context.

In the EPLI context, the results are, at best, mixed, depending on your perspective. While data suggest EPLI and the risk management services offered with the insurance policy can potentially improve employment practices and compliance, it also suggests that EPLI risk management services often shape compliance in a way that leans more toward making claims defensible rather than fostering a discrimination-free workplace. Similar to D&O insurance, the punitive and deterrence goals of anti-discrimination laws may remain unfulfilled when employers purchase EPLI and are able to pass those costs off to insurers. Moreover, too much reliance on EPLI risk management systems may allow employers to avoid more active involvement with the design, content, enforcement, and maintenance of its employment policies. By encouraging employers to use insurer-sponsored legal hotlines, insurer-sponsored contract builders, and employment handbook online portals, the insurance field shifts responsibility for hard normative judgments to others (such as insurance companies) operating outside the organization.

Finally, unlike the cyber and D&O contexts, EPLI risk management services do not just reduce risk, they actively construct the meaning of compliance and law. Given that much of employment law is ambiguous, insurance companies are filling in the space and interpreting the meaning of compliance in ways that they do not in the privacy law context. The insurance field acts as a legal intermediary between the language of civil rights caselaw and statutes and how civil rights are implemented and enforced by employers. Thus, similar to the D&O context, risk management services may merely encourage employers to reduce their exposure and liability rather than prevent discrimination, improve work culture, and cultivate a discrimination-free work environment.

The empirical turn towards studying the processes and mechanisms through which insurers act as risk regulators is important. As opposed to focusing on the forms and functions of insurance and analyzing the conditions under which insurance companies impact society, more recent empirical explorations of insurer risk management that are highlighted in this Article focus on the processes through which insurance institutions construct the meaning of compliance and law. In doing so, I widen the lens on "insurance as regulation" beyond the deterrence, moral hazard, and loss prevention focus of prior scholars. The fact that the insurance field transforms the moral logic of anti-discrimination law through a risk management filter demonstrates that the insurance-as-regulation narrative is not simply one of assessing how well liability insurance delivers law's deterrence signal. Rather, insurance as regulation is also a story of how insurance organizations *transform* that deterrence signal.

The purpose of this Article is not to suggest that insurers are not risk regulators. Given the limitations of public regulatory law and private contract law, clearly insurers are stepping in and regulating many aspects of individual's lives and how corporations operate. Moreover, this Article does not disagree with the notion suggested by insurance law scholars that insurers can help regulate corporations, encourage greater compliance, decrease moral hazard, and deter corporate misconduct. Insurers often engage in acts of regulation, in part, because there is a regulatory void. In the privacy, corporate, or employment contexts, insurers have an opportunity to bring order to a field where state regulators either have little access, mandate, or interest in regulating. Taken collectively, however, these three case studies suggest that insurance companies as corporate regulators is a much more cloudy proposition than previously thought.[155] Too often scholars celebrate insurance regulatory interventions without unpacking precisely how insurer risk management operates on the ground. Moreover, insurance company impact on corporations goes beyond policy provision and language. If these three case studies suggest anything, it is that insurer risk management interventions are not always constructive. Thus, from a policy standpoint, public legal institutions, such as courts, legislatures, and regulatory institutions, should not give so much deference to insurance company regulatory interventions without evaluating the precise way that insurer risk management techniques operate.

Insurance as regulation, therefore, should be thought of on a continuum. We must be mindful of the fact that each context is different. For example, there are important distinctions between directors and officers and cyber contexts. In the directors and officers context, directors and officers are less eager to be told how to engage in risk averse behavior. Policyholders in the cyber context, however, are in-

155. To Ben-Shahar and Logue's credit, they acknowledged that their argument on how insurance reduces moral hazard needed further evaluation in part to determine if insurers play a positive or negative role as insurers:

> [r]egulation by insurance often walks a delicate path between a socially desirable, information-rich incentive mechanism and an opportunistic set of self-serving, rent-seeking tactics. Insurers can require specific forms of conduct from their clients in order to improve safety, but they can also do this as a pretense for unjustified denial of paid-for-coverage. We don't know which pattern dominates.

Ben-Shahar & Logue, *Outsourcing Regulation*, *supra* note 7, at 248.

terested in the insurance defense and indemnity coverage but also the accompanying risk management services that can prevent, detect, and respond to a data breach event. The risk management services that accompany cyber insurance also fill a competency or knowledge gap for the organization. Organizations are willing to use risk management tools that deal with the latest cyber threats that it lacks internal tools to defend against. In contrast, directors and officers believe they possess the requisite knowledge and experience to manage a corporation responsibly and are less eager to receive insurance risk management recommendations.

There are also differences between the EPLI and cyber situations. EPLI insurers spend considerable time trying to shape the meaning of law for employers tasked with dealing with discrimination laws whereas cyber insurers spend far less time mediating law's meaning and far more time trying to enhance an organization's ability to detect and respond when faced with a data breach. Unlike in the EPLI context, the cyber insurance risk management tools are less about simply avoiding being sued and more about developing processes to prevent or limit any data breach problem from occurring. Therefore, the conditions under which insurance as regulation works depends on a variety of factors.

Moving forward, we need more empirical studies that reveal how insurer risk management services and loss prevention practices actually operate. This is crucial because insurer rules and interventions are not established after public debate, periods of comment and revision, or votes by an electoral body. Insurance company risk management is often concealed by layers of organizational routines and not always recognized as insurance rules. Insurance scholars and regulators need to explore *under what conditions* insurers act as regulatory intermediaries in ways that decrease the likelihood of moral hazard. How insurance company based deterrence plays out on the ground is much more complicated than previously suggested. Corporations are increasingly nudged toward more stakeholder models of governance that encourage broader levels of accountability to communities beyond just shareholders. Corporations increasingly rely on intermediaries due to the rise of laws impacting corporations. Through various lines of insurance, insurers play a significant role in steering organizations toward complying, or at least appearing to comply, with the many laws that regulate organizations. Given that there is variation in the extent to which insurer risk management and compliance programs embrace or neglect formal adherence to privacy, corporate, and employment laws, future studies should examine under what conditions insurers, in their capacity as risk managers, facilitate or inhibit corporate social responsibility and the goals of legal regulation.