Yale Journal of Law & Technology
Volume 28, Symposium Issue

Corporate Law's Duty of Data Loyalty

Andy Serwin,[*] Neil Richards,[**] Woodrow Hartzog,[***] and Ryan Durrie[****]

[*] Partner, DLA Piper LLP, and the U.S. Chair, and Global Co-Chair of the Data Protection, Privacy and Security Practice, and a member of the Firm's Executive Committee. Fellow, Cordell Institute for Policy in Medicine & Law, Washington University in St. Louis.
[**] Koch Distinguished Professor in Law and Director, Cordell Institute for Policy in Medicine & Law, Washington University in St. Louis.
[***] Professor of Law, Boston University. Fellow, Cordell Institute for Policy in Medicine & Law, Washington University in St. Louis.
[****] Director AI Initiatives, Co-Director WashU Law AI Collaborative, Associate Director for Policy, Cordell Institute for Policy in Medicine & Law, Washington University in St. Louis.

Article Contents

Introduction

Privacy law used to be a relatively tidy field, involving a few interesting but discrete topics like press disclosures of private facts, wiretapping, and the processing of personal data by internet companies. But as the digital revolution continues to disrupt area after area of human activity and software "is eating the world,"[1] the core concerns of privacy law such as "when is it appropriate to process personal data?" have similarly entered field after field. Today, most fields of law, including discrimination law, antitrust, and international law, have found it necessary to reckon with the questions of informational harm and power with which privacy law has been concerned in recent decades.[2]

Although personal data and privacy law have become areas of core concern in these disparate areas of law, the United States has been slow to address these issues. The United States remains the only advanced economy without a comprehensive, national data protection law providing rights to its citizens regarding how their data is processed and placing general obligations on the private entities that process that data. There have been no shortage of proposals for a federal statute, and over a dozen states have passed their own "comprehensive" privacy laws.[3] Yet as we have explored in prior work, the national debate has lacked both a consensus on what needs to be done and a set of proposals that meaningfully push the debate beyond the existing frameworks of notice (where that "notice" can be buried in a privacy policy no one reads) and choice (where the choice can be little more than the choice not

---

[1] Marc Andreessen, *Why Software Is Eating the World*, WALL ST. J. (Aug. 20, 2011), https://www.wsj.com/articles/SB10001424053111903480904576512250915629460 [https://perma.cc/DGY5-6VF6].

[2] *E.g.,* Pauline T. Kim, *Manipulating Opportunity*, 106 VA. L. REV. 867 (2020); ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD (2020); ANU BRADFORD, DIGITAL EMPIRES: THE GLOBAL BATTLE TO REGULATE TECHNOLOGY (2023).

[3] *See* INT'L ASS'N OF PRIVACY PROF'LS, *U.S. State Privacy Legislation Tracker*, IAPP (last visited Mar. 13, 2025), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ [https://perma.cc/RH84-DEWQ].

to use the internet).[4] Given the current push towards deregulation at the federal level, it appears unlikely that any national level regulation will move forward in the near term.

Recent scholarship searching for frameworks superior to the failed notice and choice model has proposed a variety of approaches, including trust-building relational approaches centered around duties of data loyalty. A significant literature has developed by scholars including Balkin, Hartzog & Richards, I. Kerr, Nissenbaum, Scholz, and Waldman.[5] Loyalty approaches have certainly had their critics, including Cohen, Grimmelman, and others, including critiques that relational models will not scale to the platform economy, that loyalty proposals are vague, and that they are contrary to existing

---

[4] In response to the Trump administration's rollback of Federal Communications Commission privacy rules in April 2017, Representative Jim Sensenbrenner stated the rationale, "Nobody's got to use the Internet." If not using the internet is a "choice," then this is an apt illustration of just how weak a "notice and choice" regime of privacy protection can be. *See* NEIL RICHARDS, WHY PRIVACY MATTERS 190 (2022). *See also* Kristine Phillips, *'Nobody's Got to Use the Internet': A GOP Lawmaker's Response to Concerns About Web Privacy*, WASH. POST (Apr. 15, 2017), https://www.washingtonpost.com/news/powerpost/wp/2017/04/15/nobodys-got-to-use-the-internet-a-gop-lawmakers-response-to-concerns-about-web-privacy/ [https://perma.cc/B9XR-33MC].

[5] Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016); Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11 (2020); Woodrow Hartzog & Neil M. Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. 985 (2022); Woodrow Hartzog & Neil M. Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687 (2020); Ian R. Kerr, *The Legal Relationship Between Online Service Providers and Users*, 35 CAN. BUS. L.J. 419 (2001); Helen Nissenbaum, *Securing Trust Online: Wisdom or Oxymoron?*, 81 B.U. L. REV. 635 (2001); Neil M. Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016); Neil M. Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961 (2021); Lauren Henry Scholz, *Fiduciary Boilerplate: Locating Fiduciary Relationships in Information Age Consumer Transactions*, 46 J. CORP. L. 143 (2020); ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE (2018); ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER (2021); ARI EZRA WALDMAN, ADVANCED INTRODUCTION TO U.S. DATA PRIVACY LAW (2023).

principles of corporate law.[6] This last critique by Khan & Pozen has been partly addressed on the merits by Andrew Tuch, but the relationships between privacy and corporate law necessary to fully examine loyalty proposals remain under-studied.[7] Moreover, Tuch's work presents yet another field that privacy has come to influence, namely substantive Delaware corporate law–a body of law that few privacy law scholars have expertise in, just as few corporate law scholars have expertise in privacy law. This is a shame, because there are important insights that privacy law and corporate law can learn from each other.

In that spirit, this Essay offers an intervention to this literature at the borders of privacy and corporate law.[8] It argues that whether or not a *privacy*-based duty of data loyalty along the lines proposed by Richards & Hartzog (and others) is a good idea, a corporate law-based duty of data loyalty already exists as part of the broader principles of Delaware fiduciary law. This corporate duty of data loyalty needs to be considered as part of the broader debate.

Our argument is developed in three steps. First, we explain the ways in which companies are already doing business using human data at virtually every level of their operations, and that this trend is only going to become more pronounced as companies invest further in artificial intelligence technologies. While these business practices justifiably alarm most privacy scholars, from the perspective of businesses—as revealed in

---

[6] Julie E. Cohen, *How (Not) to Write a Privacy Law* 2 (KNIGHT FIRST AMEND. INST. AT COLUM. UNIV., Mar. 23, 2021); James Grimmelmann, *When All You Have Is a Fiduciary*, LAW & POL. ECON. PROJECT (May 30, 2019); Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497 (2019). For a response to these (and other) critics of data loyalty, *see* Woodrow Hartzog & Neil M. Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. 985 (2022).

[7] Andrew F. Tuch, *A General Defense of Information Fiduciaries*, 98 WASH. U. L. REV. 1897, 1902 (2021) (arguing that Khan and Pozen "significantly overstate the threat that corporate and fiduciary law poses for the information fiduciary model").

[8] Portions of this paper are based upon, and in furtherance of, scholarship from one of the authors appearing in the following unpublished works: Andy Serwin, *Defining Governance in a Hybrid World* (Sept. 30, 2022) (unpublished manuscript), and Andy Serwin, *Understanding Delaware Fiduciary Duties—Putting Governance and Risk in Context and Reducing Personal Liability* (Aug. 2023) (unpublished manuscript), both available at https://laresinstitute.com/publications [https://perma.cc/6V56-TQW6].

their corporate filings, and in germinal work by Cohen and Zuboff—the collection and exploitation of personal data have become indispensable to their operations as a factual matter.[9]

Second, looking to Delaware fiduciary law, we argue that there is already a more than colorable claim that existing law mandates a kind of data loyalty: If personal data has become indispensable to businesses, then the existing Delaware duties of care and loyalty imposed on directors and officers and the *Caremark* duty of oversight apply to the provenance, legality, and sustainability of the continued use of that data. Moreover, this duty requires more than the thin notions of compliance that companies have continued to assert. The critical point here is that legal compliance is one risk, but not the only risk, that the Delaware fiduciary duty requires companies to address. If one accepts the point (advocated by companies themselves) that the vast majority of business processes depend on the use of technology and data, then it becomes clear that the duties that the directors and officers owe (care and loyalty) would inherently cover a company's use of data and digital technology. Because Delaware law requires companies to be both "compliant" and "resilient," companies have a duty to make sure that their use of data is done in a manner that is doesn't place the business at risk from foreseeable legal liability or even foreseeable changes in law.

Third, we argue that recognizing this corporate duty of data loyalty has significant advantages for privacy protection. To be sure, this duty of data loyalty is distinct from the one proposed by Richards and Hartzog in that it runs from the directors and officers to the corporation, rather than to the data subjects themselves. But it has the advantage of being (1) an existing data loyalty duty that privacy advocates can point to as precedent; and (2) a constraint on the ability of companies to rewrite privacy in self-interested ways as documented in detail by Waldman.[10] Moreover, for both corporations seeking to get ahead of resiliency risk and lawmakers seeking substantive

---

[9] JULIE E. COHEN, BETWEEN TRUTH & POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM (2019); SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019).

[10] *See* ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER (2021).

data privacy rules, there are real advantages to recognizing this corporate duty of data loyalty right now.

We conclude by arguing that a duty of data loyalty from *privacy law* may well be the ideal way to solve many of the problems of informational and platform capitalism. However, as we search for new solutions to these problems, it's time for us to recognize that there is already an existing *corporate duty of data loyalty* that can be used to begin addressing these problems without needing to change the law. Additionally, with a lack of federal action and the recent pushback against agency regulatory extension and interpretation,[11] state laws have become an increasingly important way of addressing privacy concerns.

I. The Business Data Revolution

The use, analysis, and processing of business data is no longer the sole domain of specialized companies, or even technology-focused companies more broadly. Across business models and industries, companies have come to rely more on their ability to process and understand data, including human data about their customers, potential customers, and employees. In a meaningful way, then, all companies today are technology companies, and all of them process human data.[12] This has given rise to what we term the "digital corporation", meaning a firm that is intentionally organized around continuous access to personal data across its operations, such that the absence of that access would severely constrain, and in some cases eliminate, its ability to function.

Two implications follow from this point. First, the design and maintenance of resilient data protection systems is no longer a specialized compliance concern but a foundational element of competent management. Second, the digital corporation operates at the mercy of the continued availability of lawfully obtained personal data. Its structure is not merely data-enabled but data-dependent.

---

[11] *See* Loper Bright Enterprises v. Raimondo, 603 U.S. 369, 413 (2024).

[12] Christopher Mims, *Every Company Is Now a Tech Company*, WALL ST. J. (Dec. 4, 2018), https://www.wsj.com/articles/every-company-is-now-a-tech-company-1543901207 [https://perma.cc/4WU8-GJDQ].

This transformation is not primarily a legal development. Rather, it is a change in how firms operate; one that has occurred gradually enough that many executives have not paused to name it. As one of us has put it elsewhere, the modern economy runs on a line of communication no different in structure from the roads, sea lanes, and airways that preceded it: a connective medium (the telecommunications backbone), a platform that travels along it (software and hardware), an engine that drives the platform (computing power, including artificial intelligence and machine learning), and a propellant that fuels the engine.[13] That propellant is data, and not personal data alone; data of every kind now fuels the ordinary operation of the modern firm.[14] Before the commercial internet, a company's marketing function relied on broadcast advertising and direct mail; its human resources function relied on paper applications and manager judgment; its product development function relied on episodic customer surveys and engineering intuition. Each of these functions now runs substantially on data pipelines, and the difference is not one of degree but of kind: Remove the data, and the function as currently designed simply does not operate.

The clearest illustration is marketing, where many firms have moved from mass messaging to individualized targeting built on continuously updated behavioral and transactional data. But the dependency runs deeper than the marketing function itself. Even companies whose public mission statements say nothing about data reveal, on inspection, that their strategies cannot be executed without it. Google describes its mission as organizing the world's information and making it universally accessible and useful, and generates the revenue that funds that mission by selling advertising built on the data its search and advertising products collect.[15] Meta describes its mission as giving people the power to build community, a mission that is inseparable from the platform's collection and use of user data to operate its social products and to sell the

---

[13] Andy Serwin, *Defining Governance in a Hybrid World* 13–15 (LARES INST., Sept. 30, 2022) (unpublished manuscript) (on file with author).
[14] *Id.* at 14, 19.
[15] *Id.* at 3–4 (quoting Google's stated mission and describing its AdWords and AdSense advertising programs).

advertising that funds them.[16] Neither company frames its mission explicitly in terms of data collection, yet neither could execute its stated strategy without it, which is precisely the point: For the digital corporation, data dependency is often implicit in the business model rather than stated in the mission, which is exactly why it is easy to overlook and important to name.

The same shift has occurred at the level of executive decision-making generally, independent of any particular function. Management scholarship has long recognized that the core job of an executive is to make decisions, and that doing this job well increasingly turns on the ability to gather, evaluate, and act on the right information rather than simply more of it.[17] Strategic planning, pricing, market entry, and resource allocation decisions that were once made largely on the basis of experience and periodic reporting are now made, in whole or in part, on the basis of continuously updated internal and external data. A firm that under-invests in its data infrastructure does not merely fall behind on a technology upgrade; it degrades its own capacity to make the ordinary decisions that running the business requires.

If data access has become structural to a company's business, then the loss of that access is not solely a compliance event but an operational one as well, and recent business history supplies a direct illustration. In 2021, Apple introduced a feature requiring mobile applications to obtain affirmative user consent before tracking behavior across other apps, a change that sharply reduced the advertising data available to platforms that had built their revenue models around it. Meta's own finance leadership told investors that the resulting reduction in available data would reduce the company's 2022 revenue by approximately ten billion dollars,[18] a single, disclosed, ten-figure illustration of a digital corporation whose

---

[16] *Id.* at 3.

[17] Serwin, *supra* note 13, at 30–31 (citing Kenneth R. Brousseau *et al.*, *The Seasoned Executive's Decision-Making Style*, HARV. BUS. REV. (Feb. 2006)).

[18] Salvador Rodriguez, *Facebook Says Apple iOS Privacy Change Will Result in $10 Billion Revenue Hit This Year*, CNBC (Feb. 2, 2022), https://www.cnbc.com/2022/02/02/facebook-says-apple-ios-privacy-change-will-cost-10-billion-this-year.html [https://perma.cc/XD2B-Y7DK].

strategy, and whose shareholders' returns, depend directly on the continued lawful availability of data it does not itself control. The company's response, rebuilding its advertising infrastructure to operate on less individualized data, was not a legal compliance project. It was a restructuring of core business operations made necessary by a change in data availability.[19]

The same dynamic appears whenever a data source a business has come to rely on becomes unavailable, whether because a platform changes its terms of access, a regulator restricts a category of transfer, or a vendor relationship ends. The practical lesson is the one identified at the outset of this Section: The digital corporation does not merely use data opportunistically, it has organized its operations around an assumption of continued access, which means that resilience against the disruption of that access belongs alongside financial and operational resilience as a core management concern, not a specialized compliance afterthought.[20]

II. The Delaware Duty of (Data) Loyalty

In the United States, corporations are artificial legal entities formed under the laws of one of the individual states.[21] A corporation is always subject to jurisdiction where it was formed.[22] This is particularly important for determining what set of laws are relevant for how a corporation is required to run its internal affairs. This principle, known as the "internal affairs doctrine," provides that the internal affairs of a corporation are governed by only one set of state laws.[23] The Supreme Court has been clear regarding the importance of this doctrine:

---

[19] *Id.*

[20] Serwin, *supra* note 13, at 22–26 (describing this concept as "data sustainability" and arguing that data risk should be assessed through an operational resiliency lens rather than a legal compliance lens alone).

[21] Andy Serwin, *Understanding Delaware Fiduciary Duties—Putting Governance and Risk in Context and Reducing Personal Liability* 6 (LARES INST., Aug. 2023) (unpublished manuscript) (on file with author).

[22] We are reminded here of Stephen Colbert's tongue-in-cheek aphorism that corporations are legal people and "[j]ust because someone was born in a lawyer's office and is incorporeal doesn't mean he should have no rights." *See* Charles McGrath, *How Many Stephen Colberts Are There?*, N.Y. TIMES (Jan. 4, 2012), https://www.nytimes.com/2012/01/08/magazine/stephen-colbert.html [https://perma.cc/D8U8-5EXT]; Serwin, *supra* note 21, at 7.

[23] *See, e.g.,* Edgar v. MITE Corp., 457 U.S. 624, 645 (1982).

> The internal affairs doctrine is a conflict of laws principle which recognizes that only one State should have the authority to regulate a corporation's internal affairs – matters peculiar to the relationships among or between the corporation and its current officers, directors, and shareholders – because otherwise a corporation could be faced with conflicting demands.[24]

The Court has grounded this importance in the need for investor certainty regarding what laws will govern the entity in which they invest.[25] Given the clear applicability and primacy of the internal affairs doctrine, the question becomes, which state's laws most often govern corporations. The answer to that question is "Delaware."

A. Delaware First

Delaware corporate law is the predominant law governing the internal affairs of U.S. companies. In the United States in 2022, approximately 68% of Fortune 500 companies and 79% of all U.S. initial public offerings were domiciled in Delaware.[26] In total, there are over 1.9 million business Delaware entities as of 2022.[27] Since Delaware law governs a majority of public companies (and a vast number of nonpublic companies),[28] understanding Delaware corporate law is necessary to any discussion of corporate governance and the duties directors and officers owe to their companies.

Delaware law requires that companies "be managed by or under the direction of a board of directors"[29] In most cases, the

---

[24] Edgar, 457 U.S. at 645 (citing RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 302 cmt. b, pp. 307–08 (AM. L. INST. 1971)).

[25] Cort v. Ash, 422 U.S. 66, 84 (1975) (stating that "Corporations are creatures of state law, and investors commit their funds to corporate directors on the understanding that, except where federal law expressly requires certain responsibilities of directors with respect to stockholders, state law will govern the internal affairs of the corporation.").

[26] *See* DEL. DIV. OF CORPS., *Annual Reports & Statistics*, DEL. DEP'T OF STATE (last visited May 5, 2024), https://corp.delaware.gov/stats/ [https://perma.cc/Z2ML-FKVR].

[27] *Id.*

[28] *Id.*

[29] 8 DEL. C. § 141(a) (2026).

board of directors will appoint a management team to run the company "under the direction" of the board of directors. The internal duties and obligations owed by the directors and officers to a company, including creating controls and oversight to ensure that a company is meeting its obligations to follow applicable laws, are defined by the state of entity formation's laws.[30]

There are two key duties under Delaware law that are applicable to officers and directors: the duty of care and the duty of loyalty.[31] Both of these duties are duties to the company.[32]

The duty of care is fundamentally a requirement that the officers and directors make "informed business decisions."[33] However, the law recognizes that directors must both make decisions and rely on subordinates in discharging this duty. Directors "are not required to review all information in making their decisions – only the information that is material to the decision before them. Nevertheless, in evaluating information provided to them by management, directors are expected to review the information critically and not accept it blindly."[34] The applicable standard for the duty of care is gross negligence,[35] including claims of insufficient review or investigation.[36] Decisions made by the directors and officers of a corporation regarding the running of a business are generally given deference by the courts under the business judgement rule.[37] "[S]o long as a majority of the directors have no conflicting interest […] in the decision, their decision will not later be second-guessed by a court if it is undertaken with due

---

[30] *See generally* Edgar v. MITE Corp., 457 U.S. 624 (1982).
[31] *See The Delaware Way: Deference to the Business Judgment of Directors Who Act Loyally and Carefully*, DEL. CORP. LAW, DEL. DEP'T OF STATE (last visited May 5, 2024), https://corplaw.delaware.gov/delaware-way-business-judgment/ [https://perma.cc/QD4P-FC34] [hereinafter Delaware Way].
[32] *See* Gantler v. Stephens, 965 A.2d 695, 708–09 (Del. 2009).
[33] *See Delaware Way*, *supra* note 32.
[34] *Id.*
[35] *See* Aronson v. Lewis, 473 A.2d 805, 812 (Del. 1984); *see also Delaware Way*, *supra* note 32.
[36] *See* Smith v. Van Gorkom, 488 A.2d 858, 873 (Del. 1985).
[37] *See Delaware Way*, *supra* note 32.

care and in good faith."[38] Courts review whether a director or officer has met their duty of care through the lens of the business judgement rule, as described in *Van Gorkem*:

> "Under Delaware law, the business judgment rule is the offspring of the fundamental principle[…] that the business and affairs of a Delaware corporation are managed by or under its board of directors. In carrying out their managerial roles, directors are charged with an unyielding fiduciary duty to the corporation and its shareholders."[39]

The duty of loyalty requires directors to "act in good faith to advance the best interests of the corporation and, similarly, to refrain from conduct that injures the corporation."[40]

As described in *Van Gorkem*, courts do not give directors the deference and protection of the business judgement rule where they have made an "unadvised" decision.[41] Directors and officers must prepare and inform themselves prior to making decisions. This requirement is a recognition of the fact that directors are carrying fiduciary duties and acting on the behalf of others when making these business decisions. [42]

In *In re Caremark International Inc. Derivative Litigation*, the Delaware Court of Chancery provided guidance on the level of supervision and oversight required to make informed decisions.[43] In general, the court described two types of claims that could arise from the failure to exercise appropriate supervision and oversight. First, a claim that the board failed to ensure a board-level monitoring and information reporting system is in place.[44] Second, a "red flags" claim in which the board was aware of red flags indicating corporate misconduct, yet consciously failed to act after learning of these red flags.[45]

In *Marchand v. Barnhill*, the Chancery Court framed *Caremark* as imposing "a duty 'to exercise oversight' and to

---

[38] *Id.*
[39] Van Gorkom, 488 A.2d at 872 (citations omitted).
[40] *See Delaware Way*, *supra* note 32.
[41] *Id.*
[42] Van Gorkom, 488 A.2d at 872 (citations omitted).
[43] In re Caremark Int'l Inc. Derivative Litigation, 698 A.2d 959, 971–72 (Del. Ch. 1996).
[44] *Id.* at 968–70.
[45] *Id.*

monitor the corporation's operational viability, legal compliance, and financial performance."[46] As the *Marchand* court states, "[Caremark] does require that a board make a good faith effort to put in place a reasonable system of monitoring and reporting about the corporation's central compliance risks.[47]

B. The March Towards Data Loyalty

While no Delaware court has directly recognized a duty of data loyalty, there are several decisions that indicate that Delaware courts are potentially moving towards recognizing such a duty. Some key decisions have shown the existence of these duties in areas near to data and privacy. In fact, the logical implication of these decisions is that there already exists a Delaware duty of corporate data loyalty, particularly in the context of data breaches and data protection. This section offers a reading of some relevant cases that suggest that such a conclusion is warranted.

In *Firemen's Retirement. Sys. of St. Louis v. Sorenson,* a 2021 Delaware Court of Chancery case involving a Marriott data security breach related to the acquisition of another hotel chain, shareholders of Marriott brought a derivative suit against the directors, claiming that they had "breached their duty of loyalty under *Caremark.*"[48] Specifically, the plaintiffs alleged that the directors breached their duty "by failing to conduct adequate due diligence of . . . cybersecurity technology" before the acquisition, and breached their duty after the acquisition since they "continued to operate [the acquired company's] deficient systems" and "failed to timely disclose the data breach" that occurred due to those deficiencies.[49] The plaintiffs alleged, in pertinent part, that the defendants breached their *Caremark* duty of oversight by consciously disregarding red flags about the defendants' "inadequate data protection systems."[50]

---

[46] Marchand v. Barnhill, 212 A.3d 805, 809 (Del. 2019).
[47] *Id.* at 824.
[48] Firemen's Ret. Sys. of St. Louis v. Sorenson, No. 2019-0965-LWW, 2021 WL 4593777, at *1 (Del. Ch. Oct. 5, 2021).
[49] *Id.*
[50] *Id.* at *15.

The court found that the plaintiffs did not sufficiently establish a *Caremark* claim but left open the possibility of a duty of loyalty in similar scenarios. The court held that no red flags were consciously disregarded, reasoning that even though the board was aware of the inadequate data protection systems, they had addressed the issue and attempted (though failed) to remediate it, and thus their actions do not constitute bad faith or turning a blind eye.[51] Although *Sorenson* was ultimately dismissed, the court seems to remain open to the possibility of a successful red flags *Caremark* claim regarding data security or data protection failures, stating that "Cybersecurity has increasingly become a central compliance risk deserving of board level monitoring at companies across sectors."[52]

In *Ontario Provincial Council v. Walton*, shareholders of Walmart brought an action claiming, among other things, that the defendants breached their fiduciary duty by failing to implement an information system to address "central compliance risks."[53] While the defendants won on their motion to dismiss based on timeliness, the court stated that cybersecurity might someday be a central compliance risk and listed several instances that indicate a central compliance risk, such as when a company:

> - Has an enterprise risk management system and has identified a risk as central[…]or
> - Has a mission statement or set of policies that call out an issue as a priority for the company […] or
> - Has touted the importance of and its proficiency in a particular area (such as a company that describes itself as providing "America's best first job,") When a company makes statements like the examples above, it becomes reasonably conceivable that protecting employees is a central compliance risk.[54]

---

[51] *Id.*
[52] *Id.*
[53] Ontario Provincial Council of Carpenters' Pension Trust Fund v. Walton, 294 A.3d 65, 85 (Del. Ch. 2023).
[54] *Id.* at 86 (internal citations omitted).

This directly correlates with data protection. Companies, in particular technology companies, often emphasize the importance of their privacy policies and the related customer trust given to them, and state that data privacy and security is a priority for them.[55] The Delaware Court of Chancery's central compliance reasoning in *Walton* is directly applicable to data security, supporting the claim for an existing duty of data loyalty.

The United States District Court for the District of Maryland held there was no violation of a *Caremark* duty when a corporation purportedly failed to oversee its manufacturing and research development of a COVID-19 vaccine.[56] The court reasoned that the defendant directors did not cause the corporate trauma, nor did they act in bad faith, and, therefore, did not breach their fiduciary duties. The court did, however, state

> a "*Caremark* claim arguably could be based on a failure to engage in oversight that led to a 'corporate trauma' or caused 'significant financial liability[.]'"

Thus, we can analogize a board's failure to oversee and adequately protect data that results in harm to the corporation and its shareholders, such as customers no longer using the corporation's services (resulting in a loss of revenue) to the

---

[55] *See generally* ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER (2021). *See also Privacy*, AMAZON NEWS (last visited Mar. 13, 2025), https://www.aboutamazon.com/about-us/public-policy/privacy [https://perma.cc/6QG2-UM9V] ("Many core features of the customer experience at Amazon depend on us using data responsibly and transparently."); Google LLC, *FAQ—Privacy & Terms*, GOOGLE (last visited Mar. 13, 2025), https://policies.google.com/faq?hl=en-US [https://perma.cc/WT3B-NAD2] ("We know security and privacy are important to you—and they are important to us, too. We make it a priority to provide strong security and give you confidence that your information is safe and accessible when you need it."); *Privacy & Security*, WALMART (last visited Mar. 13, 2025), https://corporate.walmart.com/privacy-security [https://perma.cc/TCH7-PG79] ("We believe that privacy is more than an issue of compliance and endeavor to manage personal information in accordance with our core value of respect for the individual.").

[56] In re Novavax, Inc. Stockholder Derivative Litigation, No. TDC-21-2996, 2023 WL 5353171 (D. Md. Aug. 21, 2023).

Maryland court's hypothetical board causing corporate trauma or significant financial liability.

Additionally, in *In re McDonald's Corp. Shareholder Derivative Litigation,* another Delaware Court of Chancery case, plaintiffs brought a *Caremark* claim for failure to oversee sexual harassment claims.[57] The court stated that "when directors fail to make any effort to establish an information system to address central compliance risks, then that failure supports an inference of bad faith."[58] The court indicated that "it is fair to infer that all 'essential and mission critical risks' necessarily qualify as 'central compliance risks.'"[59]

In *Construction Industry Laborers Pension Fund v. Bingle*, the plaintiffs sued after a software company called SolarWinds experienced a large-scale cyberattack.[60] The plaintiffs brought a *Caremark* duty of oversight claim, which the court dismissed. The court reasoned that the company did not violate "positive law" and that the plaintiffs did not sufficiently allege bad faith.[61] However, the court did not foreclose the notion that cybersecurity risks could be business risks that boards have a duty to oversee. Rather, the court stated that they "agree fully with the *Sorenson* court that good corporate practice requires director consideration of potential risks to customers; particularly so, perhaps, regarding cybersecurity."[62] Thus, the court seems to indicate a plaintiff may successfully bring a breach of duty of oversight of cybersecurity issues if they prove a "reasonable inference of scienter and therefore actions taken in bad faith by the Board."[63]

---

[57] In re McDonald's Corp. Stockholder Derivative Litigation, 291 A.3d 652 (Del. Ch. 2023).
[58] *Id.* at 679.
[59] *Id.* at 678.
[60] Construction Industry Laborers Pension Fund v. Bingle, No. 2021-0940-SG, 2022 WL 4102492 (Del. Ch. Sept. 6, 2022), *aff'd*, 297 A.3d 1083 (Del. 2023).
[61] *Id.* at *36 ("In sum, the Complaint has not pled sufficient particularized facts to support a reasonable inference of scienter and therefore actions taken in bad faith by the Board.").
[62] *Id.* at *33.
[63] *Id.* at *36.

C. Is This It?

While no court has yet held expressly that the *Caremark* duty of oversight applies to the use and protection of data held by corporations, it seems that courts are willing to consider a breach of a duty of loyalty should a plaintiff sufficiently prove bad faith and failure to oversee data. In particular, the *Sorenson* case lends support to this argument. The court there indicated the potential for failures in cybersecurity—of which data security is one of, if not the primary component—to rise to the level of being considered as failures to discharge the duty of loyalty to the company.[64] One could imagine similar challenges being presented by ransomware scenarios involving critical systems or to injunctions imposed on companies' important personal data under the GDPR's cross-border provisions under the *Schrems II* precedent from the European Court of Justice. *Ontario Provincial Council* also explicitly stated that cybersecurity/data security may be a central compliance risk over which directors and officers must exercise due care and oversight.[65]

Taking these cases as a whole, data protection could reasonably be viewed as a mission critical component (*In re McDonald's*) because of the prevalence and importance of data in most corporations (*Sorenson*), coupled with the extensive potential corporate trauma that could be caused by a data breach or misuse (*In re Novavax*), and, as such, is a central compliance risk (*Ontario*) where failure of oversight could give rise to breach of duty claims. Additionally, as we saw above, companies themselves consider customer data and privacy to be key components of their business.[66] If this duty exists, then officers and directors must weigh the balance of the risk of data breaches and other data misuse against the potential value of the data or data practice at issue. How to make that determination is a subject for a later paper.

---

[64] *See supra* note 50.
[65] *See supra* note 55.
[66] *See supra* notes 50, 55, 58–59.

III. The Privacy Virtues of Corporate Data Loyalty

Having demonstrated that Delaware corporate law already has something that we might characterize as a duty of data loyalty, this Part considers the significance and implication of such a finding. Our current thinking is that the existence of a colorable claim that Delaware corporate law imposes a duty of data loyalty suggests a number of important implications for data protection law and theory more generally. We think that there are five such implications currently.

First, of course, the potential *existence* of a duty of data loyalty within Delaware corporate law is significant on its own terms, both as a matter of corporate law doctrine and as a substantive duty for privacy and data protection law. As we have explained, firms have based their business models upon the lawful availability of personal data, the misuse or loss of which could cause a significant corporate trauma. And since Delaware corporate law places a fiduciary loyalty obligation on officers and directors to avoid substantial corporate trauma, it follows as a matter of logic that there is a fiduciary obligation to avoid such kinds of catastrophic misuse or loss of data. This means that there is a fiduciary duty of data loyalty applicable to all firms governed by Delaware corporate law, including most or all of the largest technology companies. This obligation would seem to go beyond mere compliance obligations. Rather, directors and officers would have to ensure that to the extent the processing of personal data is mission critical to a business model, foreseeable risks—such as data breaches, regulatory enforcement, and the consequences of foreseeable future laws—are sufficiently mitigated. This obligation would have particular force in cases where future data breaches, ransom attacks, or injunctions against processing might substantially curtail business operations and/or profitability.[67]

Second, the corporate duty of data loyalty is *distinct* from existing academic and legislative proposals for duties of data loyalty or to treat data processors as fiduciaries. The existing data loyalty proposals from privacy and data protection law would invariably place an obligation on those who process personal data to do so in ways that were in the best interests

[67] *See supra* notes 12–20 and accompanying text.

(or at least nor harmful to) the people whose data is being processed.[68] European data protection law would call such people "data subjects."[69] By contrast, the corporate duty of data loyalty is owed not to data subjects, but to the corporate entity itself. Another way to characterize this distinction is as follows: Existing data loyalty proposals would require a company's officers to act in the best interests of data subjects with respect to their data, whereas the corporate duty of data loyalty would require those officers to act in the best interests of the company with respect to the legal and operational risk that data subject rights pose to the continuance of resilient operations. Thus, to the extent that state or federal laws might recognize data subject loyalty rights in the future, those rights would be distinct from the corporate data loyalty obligation. However, such federal claims would nonetheless affect the corporate data duty of loyalty. For example, imagine if Congress were to pass a data subject loyalty statute. In the same way that large data breaches causing massive liability have posed operational risk in the past, those data subject loyalty rights would need to be afforded by the company or else it could face operational risk. In this way, the loyalty duties would be distinct, but they could nonetheless affect each other.

Third, the corporate duty of loyalty offers a useful *precedent* for lawmakers considering other substantive duties, particularly the duty of data loyalty we have examined in other work. Duties of data loyalty from privacy law have faced two primary obstacles. First, from the academic literature, they have been critiqued as either unworkable or incoherently vague.[70] Second, in the state legislatures, an army of tech company lobbyists have sought to worry state lawmakers that data loyalty and other substantive privacy rules are both unprecedentedly radical and hostile to corporate interests.[71]

---

[68] *See, e.g.,* Neil M. Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961 (2021).

[69] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, art. 4(1), 2016 O.J. (L 119) 1, 33.

[70] *See* IGNACIO COFONE, THE PRIVACY FALLACY: HARM AND POWER IN THE INFORMATION ECONOMY 95 (2023) (collecting examples of such critiques).

[71] *E.g.,* Jeffrey Dastin *et al.*, *Amazon Wages Secret War on Americans' Privacy, Documents Show*, REUTERS (Nov. 19, 2021),

The example of the corporate data loyalty doctrine offers a powerful response to each critique. With respect to the academic critique regarding the supposed vagueness of loyalty obligations, the long history of common law fiduciary loyalty rules demonstrates that common law processes retain the flexibility to respond to changed circumstances, technologies, and business models.[72] And with respect to the corporate critique, Delaware corporate law offers its own response to the claims of novelty, hostility, and impracticality: Officers and directors have long owed duties of loyalty to their corporate entities, and these duties are one of the bedrocks of corporate governance. It would be puzzling to suggest that a baseline principle of corporate governance is somehow unworkable or hostile to corporate governance. Moreover, to the extent that lawmakers might be skittish about imposing new substantive duties on data processors, whether out of a fear of novelty or of somehow "stifling innovation," the functional history of corporate loyalty rules shows that even broader data loyalty rules would be hardly a radical change from existing legal principles. After all, loyalty duties are not unique to corporate law, as they are close cousins to the long-standing duties that lawyers and doctors owe to their clients and patients. And everyone knows what it feels like to be betrayed, further allaying fears that data loyalty rules create rights to remedy nonexistent, hypothetical, or conjectural injuries.

Fourth, the evolution and maturation of the corporate duty of data loyalty is a sign that *data protection law will be insufficient on its own* to the project of bringing the information revolution within the rule of law in a sustainable manner. While privacy and data protection law will remain important, the problems of data and data regulation are increasingly transcending the bounds of any one body of law. Other bodies of law are likely to be essential to this project, and it is possible that some of them have not been invented yet. This finding has both descriptive and prescriptive dimensions. Descriptively, the corporate duty of data loyalty illustrates how the

---

https://www.reuters.com/investigates/special-report/amazon-privacy-lobbying/ [https://perma.cc/WY97-CKMR].

[72] Woodrow Hartzog & Neil M. Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. 985, 1013–32 (2022) (refuting this point in detail and with specificity).

information revolution represents challenges to existing law, business, and social practices that far surpass the capabilities of the traditional legal tools with which law has addressed them, such as privacy, data protection, and consumer protection law. Such a finding should not be a surprise; for example, the industrial revolution's business models spawned many new areas of law, from labor law and workplace safety to environmental law, consumer protection law, and even data protection law.[73] Normatively, it suggests that the problems of digitization will require not just the adaptation of venerable doctrines like the duty of loyalty, but the creation of entirely new bodies of law. We are fooling ourselves if we think that our existing legal doctrines and bodies of law—even those from the industrial age—are sufficient to deal with the problems of the information age. The flexibility of the duty of loyalty is a good trick, but not the only trick we need.

Fifth, there is currently uncertainty over the ability of federal regulators, such as the Federal Trade Commission, to extend or interpret regulations in novel or expansive ways.[74] Additionally, there is seemingly little appetite at the federal level for creating new regulatory schemes: in fact, the current government's appetite seems to be for *de*regulation.[75] Given the low likelihood of any federal law or regulation being promulgated, state-level action is the key remaining means for creating meaningful data protections. Looking to existing state law may in fact be the best available option for addressing privacy and data risks. It is of urgent importance that these risks are addressed, since the continued rise of AI models—and

---

[73] Woodrow Hartzog & Neil M. Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1760–61 (2020).

[74] *See generally* Loper Bright Enterprises v. Raimondo, 603 U.S. 369 (2024).

[75] *President Trump's Deregulation Effort Has Already Saved Families Thousands of Dollars*, WHITE HOUSE (Mar. 6, 2025), https://www.whitehouse.gov/articles/2025/03/president-trumps-deregulation-effort-has-already-saved-families-thousands-of-dollars/ [https://perma.cc/3H2A-RPKY] ("Upon taking office, President Trump immediately blocked these proposed rules and has initiated an aggressive deregulatory agenda that requires substantial cuts in existing regulations for each new agency rule.").

the massive increase in data processing they allow—means that the scale of these risks will only continue to grow.[76]

Conclusion

A duty of data loyalty from privacy law may well be the best way to solve many of the problems of informational and platform capitalism, but as we search for new solutions to these problems, it's time for us to recognize that (perhaps surprisingly to privacy scholars) there is already an existing duty of data loyalty from corporate law. Recognizing the connections between privacy law and corporate law suggests that some of the solutions to our pressing information-age problems might be revealed by unlikely sources. And it reveals evidence from an unlikely source that data loyalty is not as unprecedented as some of its critics might assert.

[76] *See* Woodrow Hartzog, Neil M. Richards, Ryan Durrie & Jordan Francis, *Against AI Half Measures*, 77 FLA. L. REV. (forthcoming 2026), https://scholarship.law.bu.edu/faculty_scholarship/4139/ [https://perma.cc/HJ93-N7WM] (expanding on this point in greater detail).