GONE BUT NOT FORGOTTEN: DOES (OR SHOULD) THE USE OF SELF-DESTRUCTING MESSAGING APPLICATIONS TRIGGER CORPORATE GOVERNANCE DUTIES?

LAURA PALK*

This Article examines the prevalent use of ephemeral, self-destructing messaging applications in publicly traded companies, and whether such use violates existing securities regulations, corporate preservation duties, and fiduciary obligations. Seemingly, the business judgment rule immunizes officers and directors from liability resulting from the use of transitory media, prohibiting shareholder-plaintiffs from successfully maintaining lawsuits and necessitating regulatory intervention. Current jurisprudential thought severely constrains a shareholder-plaintiff's ability successfully to hold officers and directors accountable for their lack of corporate oversight and their failure to disclose material information, including risks associated with the types of information systems a company uses in its daily operations. Regulatory intervention is needed to ensure the board, external auditors, and the trading public may assess the extent to which such media jeopardizes the company's finances, risk posture, and cybersecurity, and provide plaintiffs with a viable avenue of redress for lackadaisical oversight.

* Lecturer, Legal Studies and Accreditation and Assurance of Learning Coordinator, University of Oklahoma Price College of Business and Assistant Adjunct Professor, University of Oklahoma College of Law. Many thanks to all who provided input and guidance. In particular, I wish to thank my husband, Scott Palk for his candid comments, Professor Razook for his advice, and my family for their support.

Introduction

"This message will self-destruct in five seconds."—Mission: Impossible.[1] Or, will it? Most online users have some recognition that digital media is never truly gone and that some form of forensic recovery may be feasible.[2] The attractiveness of ephemeral digital media's transitory nature is significant.[3] Snapchat, TigerText, and Cyber Dust in varying degrees were designed to be transitory, with little to no digital trace, similar to a face-to-face discussion.[4] However, with many businesses using social media and digital communications for their daily operations, officers and directors are faced with ethical and legal issues.[5] Numerous legal requirements dictate the type of information corporations must maintain, preserve, or disclose depending on the nature of their business.[6] Ethical considerations exist regarding whether and to what extent officers should advise directors and shareholders of the daily, business use of ephemeral media.

Unlike the business world of old, employees may not all work in the same physical space, and face-to-face conversations with supervisors and colleagues are far less common.[7] Collaborative proponents argue there should be a way to tap into the transitory, digital world while maintaining the ability to have verbal conversations that may be scandalous when spoken but later become creative masterpieces.[8] Fear over scrutinized statements or ideas curbs innovation.[9] At one end of the self-destructing messaging application (referred to hereafter as "ephemeral media" or "ephemeral communi-

---

[1] Mission: Impossible (Paramount Pictures 1996).

[2] For a discussion of a computer forensic technician's ability to recover data, see *Digital Forensics and e-Discovery*, MSA Security, http://www.msasecurity.net/msa-digital-forensics (last visited Nov. 16, 2016); *see also* Michael Arnold & Dennis R. Kiker, *The Big Data Collection Problem of Little Mobile Devices*, 21 Rich. J. L. & Tech. 10 (2015).

[3] *See id.*

[4] *See* Marc Eisner, J.D., PMP, *SnapChat, CyberDust, and Confide: Disappearing eDiscovery?* (Feb. 10, 2015), https://lhediscovery.com/blog/SnapChat-CyberDust-and-Confide-Disappearing-eDiscovery.

[5] *Id.*

[6] *See* discussion *infra* Part III.

[7] *See* Kevin Maney, *Beyond Email: SnapChat, Slack, Yik Yak and Cyber Dust Are the New Frontier of Communication* (Mar. 23, 2015, 1:48 PM), http://www.newsweek.com/2015/04/03/beyond-email-snapchat-slack-yik-yak-and-cyber-dust-are-new-frontier-316031.html.

[8] *See id.*

[9] *See id.*

cations") spectrum is Cyber Dust, designed to never leave a trace of the conversation.[10] Cyber Dust communications are not stored on any servers and are fully encrypted at both ends.[11] However, an Apple device allows screenshots of Cyber Dust while an Android device does not.[12] At the other end of the transitory spectrum is Slack, which is a combination of online chat, cloud based file-sharing, and group messaging application.[13] Slack retains every item and places it in a searchable archive for later retrieval.[14]

In this Article, I explore whether the use of such ephemeral forms of communication among officers, employees, and directors violates their fiduciary duties, effectively forfeiting any protection afforded by the business judgment rule. I begin by outlining the parameters of the business judgment rule and the possibility of differing liability standards between officers and directors. Next, I discuss the cybersecurity obligations and issues associated with the use of ephemeral media, and directors' obligation to ensure they have conducted an effective information technology (IT) risk assessment. In Part III, I examine whether the use of digital media creates red flags under Securities Exchange Commission (SEC) regulations. Subsequently, I address the latest amendments to the Federal Rules of Civil Procedure regarding preservation of evidence and how the use of ephemeral communications could violate a duty to preserve and could create other records inspection

---

[10] Messages ("blasts") disappear within twenty to one-hundred seconds. *Frequently Asked Questions*, CYBER DUST, https://www.usedust.com/faqs (last visited Oct. 24, 2016). However, the user is able to pin the messages he sends and can enable his messages to be re-sent (a "reblast"). *Id.*

[11] However, according to the Cyber Dust Privacy Policy, the application advises that it collects information including *inter alia* the username, password, email address, phone number, contact list, photo rolls, the time, date, sender and recipient of the message, the number of messages sent and received, and the amount of time spent on its website, the access times, the pages viewed, and the user's IP address on its websites. *Privacy Policy* ¶ 4, CYBER DUST, https://www.usedust.com/privacy-policy (last visited Oct. 24, 2016). It also cautions the user that Cyber Dust may release the user's information in response to legal process and that unauthorized users may be able to decode its encryptions, that messages may not be deleted within a specified time frame, and that others may screenshot the messages. *Id*. at ¶ 5. In 2015, a computer forensic analyst suggested the application may leave some footprints depending on the nature of the user's device. Patrick Siewert, *Cyber Dust Claims of Privacy Debunked*, LINKEDIN PULSE (Apr. 2, 2015), https://www.linkedin.com/pulse/cyber-dust-claims-privacy-debunked-patrick-siewert-scers-bcert-lce (opining that data is actually stored on a device, and even though encrypted by Cyber Dust, the issue of recovery will be based more on the user's choice of device than on the security of the application itself, a concern to which Mr. Siewert indicates Cyber Dust has taken issue). *But see* Andra Zaharia, *The Best Encrypted Messaging Apps You Can (and Should) Use Today*, HEIMDAL SECURITY BLOG (Jun. 9, 2016), https://heimdalsecurity.com/blog/the-best-encrypted-messaging-apps/ (describing that those applications like Cyber Dust which are encrypted end-to-end as well as while in transit are the most secure messaging applications).

[12] *See Frequently Asked Questions*, CYBER DUST, https://www.usedust.com/faqs (last visited Oct. 24, 2016). *Cf.* Derek Walter, *Cyber Dust Review: Mark Cuban's Private Messaging App is Just Too Inconvenient*, GREENBOT (Aug. 7, 2014, 12:00 PM), http://www.greenbot.com/article/2462430/cyber-dust-review-mark-cubans-private-messaging-app-is-just-too-inconvenient.html (suggesting that a user can still screen shot a Cyber Dust blast on an Android).

[13] *See* SLACK, https://slack.com/is (last visited Oct. 2, 2016).

[14] *Id.*

and retention issues. Finally, I conclude with a recommendation that federal regulations and accounting guidelines should require the corporation to disclose the use of ephemeral media as a form of communication and have policies in place addressing the potential implications of such use.

This Article contributes to the current literature by examining the daily business practice of communicating through ephemeral media, which raises a variety of red flags. I posit that officers must disclose the use of ephemeral communications to their shareholders and directors. Further, the company must advise its external auditors that its employees utilize this form of communication, and the external auditors must examine whether such use interferes with corporate internal controls. Otherwise, misconduct can go undetected. Many proponents of ephemeral media argue that the use of ephemeral communications is no different from face-to-face conversations. However, face-to-face conversations rarely involve tens or hundreds of individuals without prior planning, calendar invitations, and meeting minutes, as can be the case with group chats in ephemeral media. At least with meetings, there is some evidence that a meeting took place, and typically, at least one person records the meeting.[15] If a business's leadership utilizes ephemeral media in its daily operations, how can an auditor, director, or shareholder effectively evaluate whether the corporation's mission is being furthered or hindered and whether there are appropriate IT controls? I am not suggesting the use should be prohibited. Rather, the disclosure of its use along with an internal company policy and oversight standards should be implemented. Failing such, regulations should provide meaningful relief for private plaintiffs.

Regulatory intervention is needed to ensure that the board, external auditors, and the trading public may assess the extent to which use of ephemeral communication jeopardizes the company's finances, risk posture, and cybersecurity. Such reform would also provide shareholder-plaintiffs with a viable avenue of redress for lackadaisical oversight. Current jurisprudential thought severely constrains a shareholder-plaintiff's ability to hold officers and directors accountable for their lack of corporate oversight and their failure to disclose material information to the trading public, including the risks associated with the types of information systems a company utilizes in its daily operations.

To better explain the analysis contained within this Article, the following scenario provides a backdrop to demonstrate the difficulties shareholders have suing a company's officers, directors, and auditors who utilize ephemeral media:

> *Mr. Smith invested $100,000 in the publicly traded stock of ABC, Inc., a temporary employment placement agency. ABC main-*

---

[15] *See, e.g.*, DEL. CODE ANN. tit. 8, § 142(a) (2016); MODEL BUS. CORP. ACT § 16.01(a) (COMM. ON CORP. LAWS OF THE SECTION OF BUS. LAW OF THE AM. BAR ASS'N 2010).

tains an internal database of payroll records for its employees and for several third-party companies. All of the payroll records contain personally identifiable information and the social security numbers of thousands of individuals. ABC has over twenty offices nationwide with thousands of full-time employees. ABC has been the subject of numerous employment discrimination claims and is currently defending a sexual harassment claim against Vice President Jones (VP Jones) in the state of Delaware, where it is incorporated.

ABC periodically makes required SEC financial disclosures, has an internal auditor, an audit committee, a disclosure committee, five directors, ten executive officers, and twenty lower-level managerial officers. Because of the nature of their nationwide business and their reticence to commit anything to writing, all of the managerial employees and officers utilize ephemeral media on their personal Apple and Android devices to discuss business, rather than emailing, texting, video conferencing, or meeting in person. Each year, an external auditor examines ABC's information control systems. The officers and directors advise the auditor and their board about the database and the cybersecurity protections in place. However, they fail to disclose how they communicate on a daily basis and what they communicate in the ephemeral media—they do not have a policy for record retention or cybersecurity protections related to personal devices used at work.

Unfortunately, VP Jones' device has been hacked, allowing the hacker to control his device and access its data, including access to ABC's payroll records. ABC's board learns of the attack one month after its occurrence and recommends that VP Jones wipe his phone and that ABC delete all personal information from its current platform and transfer it onto an encrypted platform according to nationally accepted best practices. Word of the breach is leaked to the public, causing ABC's stock to drop in value from $20 to $1 per share. The board decided not to disclose the breach on its financials as it had yet to be sued or investigated for the breach.

Mr. Smith and ABC shareholders sue the board in a derivative action for the board's and officers' breach of oversight duty and for the officers' negligence in exposing the company to cybersecurity attacks, invasion of privacy, and litigation spoliation claims. As examined below, these shareholder-plaintiffs face a daunting hurdle despite the clearly negligent behavior of the officers and directors.

I. Who's Minding the Store?

Publicly traded companies are obligated to maximize shareholder wealth. But in reality, who is managing the corporation and whose interests are they serving? Corporate entities, both public and private, are created and governed by the laws of their state of incorporation.[16] It is no surprise that a corporate entity seeks to incorporate in a state that is favorable to the corporate entity.[17] Historically, this has been the state of Delaware.[18] Of the Fortune 500 companies in the United States, over 65% are incorporated in Delaware.[19] Legal scholars have argued that Delaware corporate law favors management's interests over the interests of shareholders,[20] an issue Delaware disputes.[21]

State law governs the creation and management of corporate entities, but there is increasing federal regulatory oversight, particularly for publicly traded companies.[22] The directors manage the company but not its day-to-day operations and should not be implicated with detailed knowledge of the company.[23] Although directors are required to manage the company in the best interests of the company and its shareholders,[24] a shareholder's ability to ensure compliance with this obligation is severely limited even in situations that a reasonable person would deem constitute gross incompetence or ineptitude.

A. Shareholders' False Sense of Security: Directors are Rarely Held Accountable

Shareholders may mistakenly believe that if corporate managers mismanage the company by dereliction of duty or incompetence, the sharehold-

---

[16] *See* Frederick Tung, *Before Competition: Origins of the Internal Affairs Doctrine*, 32 J. Corp. L. 33, 35 (2006) (noting disputes related to the relationship between shareholders and a company's directors or the internal operations of the corporation are governed by the laws of the state of incorporation).

[17] *See id.* at 42–43.

[18] *See id.*

[19] *Benefits of Incorporating in Delaware*, DelawareInc.com, https://www.delawareinc.com/before-forming-your-company/why-delaware/ (last visited Oct. 26, 2016).

[20] *See Facts and Myths*, http://corplaw.delaware.gov/eng/facts_myths.shtml (last visited Oct. 26, 2016).

[21] *Id.*

[22] *See* E. Norman Veasey, *State-Federal Tension in Corporate Governance and the Professional Responsibilities of Advisors*, 28 J. Corp. L. 441, 443 (2003) (focusing on Delaware law).

[23] *See, e.g.*, Robert W. Hamilton, *Corporate Governance in America 1950-2000: Major Changes But Uncertain Benefits,* 25 J. Corp. L. 349, 363–64 (2000) (day-to-day operations are handled by a company's employees).

[24] *See also* William T. Quillen, *The Federal-State Corporate Law Relationship - A Response to Professor Seligman's Call for Federal Preemption of State Corporate Fiduciary Law*, 59 Brook. L. Rev. 107, 128 (1993).

ers can hold the corporate managers accountable for their losses.[25] There are times when a director fails or refuses to enforce a duty owed to the company, and the shareholder will pursue a derivative suit on behalf of the company.[26] To successfully pursue an action against a company's board of directors, the shareholder must demonstrate that a director breached his fiduciary duty to the corporation.[27]

A director's fiduciary duty to the company includes a duty of care[28] and a duty of loyalty.[29] Nonetheless, Delaware allows a company's articles of incorporation to limit directors' liability by exculpating them from their duty of care.[30] However, despite the exculpation permission, companies may not waive a director's duty of loyalty, which contains a concomitant duty of good faith that a director informs himself of all available facts prior to making a decision.[31] In analyzing how a director might breach his fiduciary duty, a court examines whether the director breached the duty because the director

---

[25] *See* Janet E. Kerr, *The Financial Meltdown of 2008 and the Government Intervention: Much Needed Relief or Major Erosion of American Corporate Law? The Continuing Story of Bank of America, Citigroup, and General Motors*, 85 ST. JOHN'S L. REV. 49, 83 (2011) (noting many states have taken Delaware' lead and permit a company's Articles of Incorporation to exculpate directors from their duty of good faith, limiting shareholders' ability to sue); Seletha R. Butler, *All on Board! Strategies for Constructing Diverse Board of Directors,* 7 VA. L. & BUS. REV. 61, 68 (2012) (discussing shareholders' lack of success in derivative suits).

[26] *See* Aronson v. Lewis, 473 A.2d 805, 811 (Del. 1984) (discussing demand futility and the interplay with the business judgment rule), *overruled on other grounds by* Brehm v. Eisner, 746 A.2d 244 (Del. 2000); Rales v. Blasband, 634 A.2d 927, 932 (Del. 1993) (detailing demand futility in oversight claims). Derivative actions are shareholder actions against a corporation. *See, e.g.*, Carter v. Hilliard, 970 N.E.2d 735, 747–48 (Ind. Ct. App. 2012) Prior to filing suit, a shareholder-plaintiff must make a demand of the board to take action against the third party on behalf of the company or specifically plead that the board refused to take action on behalf of the company or that it would have been futile to make such a demand. *Id.*

[27] *See, e.g.*, *Aronson*, 473 A.2d at 811; *Rales*, 634 A.2d at 932.

[28] *See In re.* Walt Disney Co. Derivative Litig., 906 A.2d 27, 60–62 (Del. 2006)*; see also* Dalia T. Mitchell, *Status Bound: The Twentieth Century Evolution of Director's Liability*, 5 N.Y.U. J. L. & BUS. 63, 146 (2009).

[29] The duty of loyalty requires directors to act in good faith in the best interests of the company and not "appear on both sides of a transaction nor expect to derive any personal financial benefit from it in the sense of self-dealing, as opposed to a benefit which devolves upon the corporation or all stockholders generally." *Aronson*, 473 A.2d at 812.

[30] DEL. CODE ANN. tit. 8, § 102(b)(7) (2016); *see* Smith v. Van Gorkum, 488 A.2d 858, 872 (Del. 1985) (holding directors must ensure they "inform[ ] themselves prior to making a business decision, of all material information reasonably available to them"), *overruled on other grounds by* Gantler v. Stephens, 965 A.2d 695 (Del. 2009); s*ee also* Emerald Partners v. Berlin, 787 A.2d 85, 96 (Del. Ch. 2001) (discussing the exculpation legislation of DEL. CODE ANN. tit. 8, § 102(b)(7) (2011)). Exculpation does not shield a director for "claims based on fraudulent, illegal or bad faith conduct. . . ." *In re* Johnson & Johnson Derivative Litig., 865 F. Supp. 2d 545, 559 (D.N.J. 2011) (internal citations and quotations omitted).

[31] *See In re* Citigroup Inc. S'holder Derivative Litig., 964 A.2d 106, 124 (Del. Ch. 2009); *see also In re* Walt Disney Co. Derivative Litig., 906 A.2d 27, 60–62 (Del. 2006) (finding directors must be "fully informed of all material facts"). A plaintiff must plead sufficient facts demonstrating that an outside director who is exculpated from monetary liability "harbored self-interest adverse to the stockholders' interests, acted to advance the self-interest of an interested party from whom they could not be presumed to act independently, or acted in bad faith." *See In re* Cornerstone Therapeutics Inc., Stockholder Litig., 115 A.3d 1173, 1180 (Del. 2015).

took an action or failed to take an action.[32] The analysis of action versus inaction dictates the court's standard of review: the business judgment rule, entire fairness standard, or lack of good faith.[33]

A court could view a board's failure to implement a policy regarding the use of ephemeral communications as taking an action by actively deciding not to have a policy because it requires corporate expense and thus is protected by the business judgment rule.[34] Or, it could be viewed as a failure to oversee the risk assessment of the entity, and constitute a *Caremark* failure-to-monitor claim.[35] No *Caremark* liability claims exist unless a plaintiff specifically shows the board willfully disregarded its fiduciary duties by completely failing to implement *any* compliance system, no matter how ineffective, or failing to respond to obvious red flags of corporate misconduct.[36]

Where the director takes an action or engages in decision-making, the business judgment rule immunizes him from liability so long as the director was disinterested[37] and independent[38] in the transaction. The business judgment rule presumes the board rendered its decision by exercising due care, requiring a plaintiff bear the burden of proving that the director was interested in the transaction, was not independent, or breached his fiduciary duty.[39] The policy rationale for this high bar is to encourage board membership by qualified individuals without fear of personal liability.[40] In applying the business judgment rule, a court simply asks if the board's decision was "rational in the sense of being one logical approach to advancing the corpo-

---

[32] *See* Edwin W. Hecker, Jr., *Fiduciary Duties In Business Entities Revisited*, 61 U. KAN. L. REV. 923, 934–35 (2013).

[33] *See generally id.*

[34] *See generally* Virginia H. Ho, *Risk-Related Activism: The Business Case for Monitoring Nonfinancial Risk*, 41 J. CORP. L. 647, 659 (2016) (making the case for financial and nonfinancial risk assessments and ensuring proper corporate performance and shareholder benefits).

[35] *See* Hecker, *supra* note 32 at 935–39, n.87.

[36] *Id.*

[37] A director is not disinterested or independent if he (1) "received a personal benefit from his or her action or inaction," or (2) "is under the control of another Board member and fails to exercise independent judgment," or (3) "faces a substantial likelihood of personal liability for the challenged action or inaction" and cannot "fairly represent the corporation's interests." *In re* Johnson & Johnson Derivative Litig., 865 F. Supp. 2d 545, 559 (D.N.J. 2011).

[38] Further, "[a] director is independent if he can base his decision 'on the corporate merits of the subject before the board rather than extraneous considerations or influence.'" *Id.* (quoting *In re* Veeco Instruments Inc., Sec. Litig., 434 F. Supp. 2d 267, 275 (S.D.N.Y. 2006)).

[39] *See, e.g.*, *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 967 (Del. Ch. 1996). To survive a dismissal under the business judgment rule, the plaintiff bears the burden of pleading particularized facts. *See, e.g.*, FED. R. CIV. P. 23.1; DEL. CH. R. 23.1; *Johnson & Johnson*, 865 F. Supp. 2d at 559. In its initial pleadings, a plaintiff must demonstrate that a director "breached their fiduciary duties, acted in bad faith or that the directors made an 'unintelligent or unadvised judgment,' by failing to inform themselves of all material information reasonably available to them before making a business decision." *In re* The Walt Disney Co. Derivative Litig., 907 A.2d 693, 756 (2005) (internal citations omitted).

[40] *See* Veasey, *supra* note 22, at 444; *see also* Lisa M. Fairfax, *Spare the Rod, Spoil the Directors? Revitalizing Directors' Fiduciary Duty Through Legal Liability*, 42 HOUS. L. REV. 393, 450 (2005) (discussing the variety of legal, corporate, and academic debate regarding directors' legal liability and the extent to which they should be held accountable for their actions or inactions).

ration's objectives."[41] It is "[o]nly when a decision lacks any rationally conceivable basis" that a court will determine there has been some bad faith and breach of fiduciary duty, warranting a disregard of the business judgment rule and individual liability.[42] If a plaintiff alleges sufficient facts to overcome the application of the business judgment rule, the board must then demonstrate the action was entirely fair to the company and its shareholders.[43] To find a breach of the duty of care and to overcome the business judgment rule's protection, the court reviews the director's actions under a gross negligence standard: " 'reckless indifference to or a deliberate disregard of the whole body of stockholders' or 'actions which are without the bounds of reason.' "[44]

Shareholders alleging a director failed to act by not overseeing a company because of the use of ephemeral communications must allege a lack of good faith,[45] a subset of the director's duty of loyalty.[46] These claims are branded *Caremark* liability claims, which are considered the most difficult of the fiduciary duty cases to win.[47] Plaintiffs must demonstrate that the board utterly failed "to attempt to assure a reasonable information and reporting system exists."[48] However, it is certainly unreasonable to assume that a director's good faith obligation requires that he possess specific information about all aspects of the company.[49] While directors may rely on man-

---

[41] *See In re* Trados Inc. S'holder Litig., 73 A.3d 17, 43 (Del. Ch. 2013) (internal citations and quotations omitted).

[42] *See In re* Orchard Enters., Inc. S'holder Litig., 88 A.3d 1, 34 (Del. Ch. 2014).

[43] *See, e.g.*, *In re* Cornerstone Therapeutics Inc., Stockholder Litig., 115 A.3d 1173, 1180 n.28 (Del. 2015) (citing *Trados*, 73 A.3d at 44). The entire fairness standard requires fairness in the substance and process of the transaction. *See* Americas Mining Corp. v. Theriault, 51 A.3d 1214, 1244 (Del. 2012).

[44] *See Walt Disney*, 907 A.2d at 750 (quoting Tomczak v. Morton Thiokol, Inc., Civil Action No. 7861, 1990 Del. Ch. LEXIS 47, at *35 (Apr. 5, 1990)).

[45] Because the theory that a director must fully inform himself of the available information is subsumed within his duty of care, and because the duty of care can be, and often is, exculpated in the articles of incorporation, a shareholder must allege a separate duty has been breached. *See* Hecker, *supra* note 31, at 954 (discussing *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 971 (Del. Ch. 1996) and Stone v. Ritter, 911 A.2d 362, 369 (Del. 2006)). Courts have determined this duty is a duty of good faith and contained within a duty of loyalty. *Id.* This is a high standard to meet.

[46] *Id.* The analysis of a director's lack of good faith is often carried out in an initial motion to dismiss regarding demand futility. *See* Rales v. Blasband, 634 A.2d 927, 934 (Del. 1993); *see also* Gabriela Jara, *Following on the Foreign Corrupt Practices Act: The Dynamic Shareholder Derivative Suit*, 63 DUKE L. J. 199, 209 (2013). Thus, to establish a failure to oversee claim, a plaintiff must allege the "red flags" the directors knew about and ignored. *See In re* Citigroup Inc. S'holder Derivative Litig., 964 A.2d 106, 134 n.93 (Del. Ch. 2009); *see also* Martin Petrin, *Assessing Delaware's Oversight Jurisprudence: A Policy and Theory Perspective*, 5 VA. L. & BUS. R. 433, 450–56 (2011) (discussing oversight liability history and challenges for shareholders).

[47] *Caremark*, 698 A.2d at 967.

[48] *Citigroup*, 964 A.2d at 122 (citing *Caremark*, 698 A.2d at 971).

[49] *Caremark*, 698 A.2d at 971.

agement to make managerial decisions,[50] there must be some minimum oversight bar set for a director to satisfy his obligations to the trading public. In changing technological times, not imposing a duty on directors to inquire about daily communications strictly limits a plaintiff's ability to demonstrate the directors "knew that they were not discharging their fiduciary duties" and consciously chose to take no action even in light of red flags or the inability to detect red flags.[51]

Because of the near impossibility for shareholder litigation success, legal scholars encourage courts to analyze *Caremark* liability cases through a different lens.[52] They suggest an assessment of reasonableness in a manager's decision and its impact on the risk to the corporation, or an assessment of how managers oversee internal risk management.[53] This Article espouses the view that utilizing ephemeral media for the business's daily operation is an intentional disregard of fiduciary duties. However, for this to be a viable claim, regulatory guidance must reflect that the use of ephemeral communication by directors and officers raises serious red flags. The use of transitory media might trigger a failure to monitor, a failure to disclose, or a failure to preserve, if it is used to shield officers, directors, and employees from liability, rather than to maximize the value of the corporation and its shareholders.[54] Current jurisprudential guidance, however, negates a shareholder's ability to hold a director accountable for what should constitute a classic case of mismanagement—the board's failure fully to understand the types of media that officers and employees utilize and the types of risks associated with such use.

B. If Director Liability is a Myth, Officers Should be Held Accountable for Oversight Liability

One might assume that if directors are immune from liability, then officers who manage the company bear a greater risk of liability for the misuse of ephemeral media. Unfortunately, one would be mistaken. The day-to-day

---

[50] *In re* HealthSouth Corp. S'holders Litig., 845 A.2d 1096, 1107 (Del. Ch. 2003), *aff'd*, 847 A.2d 1121 (Del. 2004) (finding directors are entitled to rely on management's preparation of financial statements in making their business decisions).

[51] *See* Desimone v. Barrows, 924 A.2d 908, 940 (Del. Ch. 2007) (citing Stone v. Ritter, 911 A.2d 362, 370 (Del. 2006)). *But see In re* SFBC Int'l, Inc. Sec. & Derivative Litig., 495 F. Supp. 2d 477, 485 (D.N.J. 2007) (finding director misconduct and the company's exculpation clause did not shelter the director's bad faith from liability). Even assuming the directors know management utilizes ephemeral media, a potential "red flag" in and of itself "do[es] not support a reasonable inference that the director defendants' [failure to act] was not in good faith." *In re* Johnson & Johnson Derivative Litig., 865 F. Supp. 2d 545, 559 (D.N.J. 2011) (internal citations and quotations omitted).

[52] *See, e.g.*, Christopher M. Bruner, *Is the Corporate Director's Duty of Care a "Fiduciary" Duty? Does it Matter?*, 48 WAKE FOREST L. REV. 1027 (2013).

[53] *See* Christine Hurt, *The Duty to Manage Risk*, 39 J. CORP. L. 253, 293 n.29 (2014) (discussing reasonable oversight versus lack of oversight).

[54] See Lyondell Chem. Co. v. Ryan, 970 A.2d 235, 240 (Del. 2009) (quoting *Stone*, 911 A.2d at 369).

operations of the corporation are delegated to the company's officers and employees, rather than controlled by the directors themselves.[55] Officers owe the same fiduciary duties to the corporation as the directors.[56] Among the officers' duties is the obligation to provide the directors with the information they need to make decisions.[57] Scholars debate the origin of these fiduciary duties.[58] Like directors, officers may be entitled to the protections of the business judgment rule and potentially the *Caremark* liability standards.[59] Whether a court should judge officers' decisions under a gross negligence standard rather than a lower ordinary negligence standard[60] is the subject of scholarly debate.[61]

---

[55] *See* Megan Wischmeier Shaner, *Officer Accountability*, 32 GA. ST. UNIV. L. REV. 357, 361 (2016).

[56] *See* Gantler v. Stephens, 965 A.2d 695, 708–09 (Del. 2009) ("Although legislatively possible, there currently is no statutory provision authorizing comparable exculpation of corporate officers."). Officers in Delaware and those states that have not adopted the Model Business Corporation Act (MBCA) or a statutory variance of the MBCA, are governed by common law fiduciary duties. Kevin G. Hroblak, *Considerations for Directors and Officers of Distressed Companies*, *in* BEST PRACTICES FOR ADDRESSING PROFESSIONAL LIABILITY CLAIMS: LEADING LAWYERS ON PROTECTING AGAINST MALPRACTICE CLAIMS AND KEEPING UP WITH CHANGING REGULATIONS, 2015 WL 1802934, at *4 (2015).

[57] *See* Amalgamated Bank v. Yahoo, 132 A.3d 752, 781 (Del. 2016); *see also* ALAN S. GUTTERMAN, BUSINESS TRANSACTIONS SOLUTIONS § 33:96 (2016) (specifying that officers have an obligation to inform the board or relevant committee of material information).

[58] *See* Megan Shaner, *The (Un)enforcement of Corporate Officers' Duties*, 48 U.C. DAVIS L. REV. 271, 297, n.104 (Nov. 2014) (citing A. Gilchrist Sparks, III & Lawrence A. Hamermesh, *Common Law Duties of Non-Director Corporate Officers*, 48 BUS. LAW. 215 (1992)) (equating officers' fiduciary duties with those owed by the directors); Amitai Aviram, *Officers' Fiduciary Duties and the Nature of Corporate Organs*, 2013 ILL. L. REV. 763 (arguing that officers can be categorized as either corporate organs or corporate agents); Lyman P.Q. Johnson & David Millon, *Recalling Why Corporate Officers Are Fiduciaries*, 46 WM. & MARY L. REV. 1597 (2005) (espousing that officers' fiduciary duties are based on agency principles); *see also* Megan Shaner, *Officer Accountability*, 32 GA. ST. UNIV. L. REV. 357, 370–71 (2016) (noting limited court decisions regarding the extent of officer liability raises issues as to their fiduciary duty parameters).

[59] *See* Shaner, *The (Un)enforcement*, *supra* note 58, at 298.

[60] *Id.* at 298 n.109. Gross negligence is generally characterized as "substantially and appreciably higher in magnitude and more culpable than ordinary negligence." *In re* AgFeed USA LLC, 546 B.R. 318 (Bankr. Del. 2016).

[61] For examples of the debate over the standard of review, see Paul Graf, *A Realistic Approach to Officer Liability*, 66 BUS. LAW. 315 (2011); Johnson & Millon, *supra* note 58; Lawrence A. Hamermesh & A. Gilchrist Sparks III, *Corporate Officers and the Business Judgment Rule: A Reply to Professor Johnson*, 60 BUS. LAW. 865 (2005); Lyman P.Q. Johnson, *Corporate Officers and the Business Judgment Rule*, 60 BUS. LAW. 439 (2005); A. Gilchrist Sparks, III & Lawrence A. Hamermesh, *Common Law Duties of Non–Director Corporate Officers*, 48 BUS. LAW. 215 (1992). For examples of scholarly analyses addressing other aspects of the officer's role as corporate agent, see Megan Shaner, *The (Un)Enforcement of Corporate Officers' Duties*, 48 U.C. DAVIS L. REV. 271 (2014); Amitai Aviram, *Officers' Fiduciary Duties and the Nature of Corporate Organs*, 2013 U. ILL. L. REV. 763 (2013); Megan Shaner, *Restoring the Balance of Power in Corporate Management: Enforcing an Officer's Duty of Obedience*, 66 BUS. LAW. 27 (2010); Donald C. Langevoort, *Agency Law Inside the Corporation: Problems of Candor and Knowledge*, 71 U. CIN. L. REV. 1187 (2003); *see also* Clark W. Furlow, *Good Faith, Fiduciary Duties, and the Business Judgment Rule in Delaware*, 2009 UTAH L. REV. 1061, 1066–67 (2009).

The very nature of ephemeral communications restricts the ability to have fully-informed decisions.[62] Where a company's officers have a policy of discussing company business through a means that self-destructs, a board cannot effectively monitor whether illegal or fraudulent activity occurs.[63] A chosen method of communication is certainly an internal affair of a corporation.[64] If that method of communication creates "a sustained or systematic failure of the board to exercise oversight[,]" shareholders should be able to hold an officer accountable for a breach of loyalty and good faith.[65] Similar to proving a breach of fiduciary duty, shareholders face a herculean battle.

If courts were to apply analogous standards as those applied to directors, then the shareholders must prove that the company did not have a risk-management system in place and was on notice regarding significant red flags.[66] Thus, even the most rudimentary and ineffective system satisfies these virtually impotent standards. Courts are reluctant to find directors liable for mismanagement that does not rise to the level of a criminal violation.[67] A divergent view ought to apply to officers—after all, they manage the company's day-to-day operations and are responsible for setting the tone and policies of the working environment.[68] Officers are more aware of the manner in which their employees communicate and whether that communi-

---

[62] *See generally* Lisa L. Casey, *Twenty-Eight Words: Enforcing Corporate Fiduciary Duties Through Criminal Prosecution of Honest Services Fraud*, 35 DEL. J. CORP. L. 1, 25–26 (2010); Thad A. Davis et al., *The Data Security Governance Conundrum: Practical Solutions and Best Practices for the Boardroom and the C-Suite*, 2105 COLUM. BUS. L. REV. 613, 637, 649 (2015) (noting the United States Department of Homeland Security is the lead enforcement agency for internal United States data breaches, and argues that it is imperative for companies to have a full understanding of their data, and their vulnerabilities arising from key employees within the company).

[63] *See* Anne Tucker Nees, *Who's the Boss? Unmasking Oversight Liability Within the Corporate Power Puzzle*, 35 DEL. J. CORP. L. 199, 240 (2010). Professor Nees suggests a five-factor test to determine whether a board should be held liable for a failure to detect illegal activity: "(1) the potential harm to the company, (2) the time [directors had] to react, (3) the source of the red flag, (4) [the] frequency [of the red flag], and (5) the availability of [relevant] information [to the directors]." *Id.*

[64] *See* VantagePoint Venture Partners 1996 v. Examen, Inc., 871 A.2d 1108, 1113 (Del. 2005) (discussing the parameters of the internal affairs doctrine).

[65] *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 971 (Del. Ch. 1996) (providing as an example an "utter failure to attempt to assure a reasonable information and reporting system exists").

[66] *See In re* Citigroup Inc. S'holder Derivative Litig., No. 07 Civ. 9841, 2009 WL 2610746, at *6 (S.D.N.Y. Aug. 25, 2009) (applying Delaware Law and stating that the board had a system in place in its "Audit & Risk Management Committee"); *In re* Am. Int'l Grp., Inc. Derivative Litig., 700 F. Supp. 2d 419, 437 (S.D.N.Y. 2010) (finding warnings about market difficulties insufficient to establish knowledge of a risk); *In re* China Agritech, Inc. S'holder Derivative Litig., C.A. No. 7163-VCL, 2013 WL 2181514, at *20 (Del. Ch. Feb. 21, 2013) (noting that it is rare a plaintiff can meet the rigorous pleading requirements for an oversight claim).

[67] *See In re* Am. Int'l Grp., Inc. Consol., 965 A.2d 763, 798–99 (Del. Ch. 2009) (holding boards' failure to monitor obvious fraud resulted in a form of criminal enterprise); Central Laborers' Pension Fund v. Dimon, No. 14-4516-CV, 2016 WL 66501, at *4–5 (2d Cir. Jan. 6, 2016) (noting to satisfy the failure to oversee threshold, a plaintiff must allege that *no* reporting system existed which resulted in a failure to detect the Ponzi scheme).

[68] *See* Shaner, *Officer Accountability*, *supra* note 58, at 361.

cation complies with legal obligations.[69] Certainly, the use of ephemeral media, social media, and personal devices is increasingly relevant for a variety of reasons, not the least of which is exposure to cybersecurity risks and SEC regulations.[70]

Formulating an appropriate standard of review for an officer's failure to implement internal data use policies and properly advise the board does not require legal gymnastics. Rather, officer liability is rooted in agency principles even if not clearly articulated as such.[71] When officers fail to implement adequate internal cybersecurity and data use policies or fail to inform themselves and their boards of the risks associated with such use, a lower standard of review is warranted. Courts should impose an ordinary negligence standard of review rather than a gross-negligence or bad-faith standard because officers have an affirmative duty to protect corporate assets from widespread and well-known cybersecurity threats. If courts immunize officers from liability simply because the officers quickly implement shallow policies with no real oversight, there is no incentive for progress.[72] At a minimum, courts should incentivize active assessment of corporate communications based on nationally accepted best practices discussed below, and allow shareholders to hold officers and directors liable when they fail to follow these best practices.

---

[69] *See* GUTTERMAN, *supra* note 57.

[70] *See, e.g.*, Fairfax, supra note 39, at 408–09 (2005) ("[S]cholars agree that the procedural rules related to derivative suits severely limit the ability of shareholders to bring legal actions to impose liability on directors for violating their fiduciary duty.").

[71] *See* GUTTERMAN, *supra* note 57 (discussing § 8.42(a) of the Model Business Corporation Act and the Restatement of Agency).

[72] *See* Kevin G. Hroblak, *supra* note 56, at *4 (2015), Lyman P.Q. Johnson, *Corporate Officers and the Business Judgment Rule,* 60 BUS. LAW. 439 (2005). *But see generally* Iron Workers Mid-South Pension Fund v. Davis, 93 F. Supp. 3d 1092, (D. Minn. 2015) (noting courts' division regarding whether officers are liable for gross negligence in the breach of their duty of care or subject to the higher standard of bad faith and conscious disregard, but assuming without deciding that "gross negligence" is the proper burden); *see also* Shaner, *Officer Accountability, supra* note 58, at 370, n.128 (discussing case law and literature regarding the ordinary versus gross negligence debate). Many argue that to encourage competent board and officer membership, their individual liability must be limited. *See, e.g.*, Mary Siegel, *The Illusion of Enhanced Review of Board Actions*, 15 U. PA. J. BUS. L. 599, 603–04 (2013) (detailing rationales for limiting the liability of directors). In reality, the incentive for membership is more likely based on the compensation packages. *See* Larry E. Ribstein, *Why Corporations?,* 1 BERKELEY BUS. L.J. 183, 199–200 (2004) (recognizing that shareholders have little voice in executive compensation, and thus, there is no realistic officer accountability). *See generally* Robert B. Thompson & Paul H. Edelman, *Corporate Voting*, 62 VAND. L. REV. 129, 144–49 (2009) (suggesting a balance between centralized management through an officer's control and accountability are warranted).

II. Managerial Oversight Should Include Cybersecurity Risk Assessment, But Currently Lacks Judicial Support

Boards and officers have a fiduciary obligation to be adequately informed about the company's IT systems and vulnerabilities.[73] The business judgment rule is designed to protect against claims of gross mismanagement even where predicated on inadequate internal controls so long as there is an absence of bad faith.[74] In this regard, a fiduciary duty is meaningless without individual accountability. The "Veracode 2015 State of Software Security Report" identified the top ten industry standard web application vulnerabilities that companies must routinely address.[75] If a company's data is breached based on one of these vulnerabilities,[76] this should trigger liability for an officer's or director's failure to monitor when nothing was done to address these issues in advance of the attack.[77]

---

[73] *See* Nishani Edirisinghe Vincent & Julia L. Higgs, *The Role of the Internal Auditor in IT Risk Management*, Internal Auditing (2016).

[74] *Id.*; *see also In re* Anderson, Clayton Litig., 519 A.2d 669, 675 (Del. Ch. 1986) (holding the business judgment rule does not apply where there are allegations of directors failing to properly disclose information to shareholders for a proxy solicitation); Miller v. Am. Tel. & Tel. Co., 507 F.2d 759, 762 (3d Cir. 1974) (finding the business judgment rule provides no protection for directors if they willfully violate a federal statute); Wolf v. Frank, 477 F.2d 467, 477 (5th Cir. 1973); *In re* Westinghouse Securities Litigation, 832 F. Supp. 989, 998 (W.D. Pa. 1993) (noting the business judgment rule protects directors from liability for poor judgment even in the context of insufficient internal controls). *Caremark* liability is triggered only when the issue rises to the level of bad faith. *See* discussion *supra* notes 45 & 46.

[75] *OWASP Top 10 Vulnerabilities*, Veracode, http://www.veracode.com/directory/owasp-top-10 (last visited Nov. 20, 2016). The Open Web Application Security Project (OWASP) is a non-profit organization dedicated to providing unbiased, practical information about application security.

[76] *See, e.g.*, Nicole Perlroth and David Gelles, *Russian Hackers Amass Over a Billion Internet Passwords*, New York Times (Aug. 5, 2014), http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html; Sara Peters, *15-Year Old Arrested for TalkTalk Attack*, Dark Reading (Oct. 26, 2015 05:30 PM), http://www.darkreading.com/attacks-breaches/15-year-old-arrested-for-talktalk-attack/d/d-id/1322836. Both the JPMorgan Chase Corporate Challenge website and the British TeleCom company were breached through one of the Top 10 vulnerabilities. *See* NYSE Governance Services, A 2015 Survey Report: Cybersecurity and Corporate Liability: The Board's View, https://www.nyse.com/publicdocs/Veracode_Survey_Report_Cybersecurity_Corporate_Liability.pdf.

[77] NYSE Governance Services, A 2015 Survey Report: Cybersecurity and Corporate Liability: The Board's View, https://www.nyse.com/publicdocs/Veracode_Survey_Report_Cybersecurity_Corporate_Liability.pdf.

According to the Ponemon Institute, the cost of cyber crime exceeds $7.7 million annually for companies. Ponemon Institute 2015 Cost of Data Breach Study: *Global Analysis*, https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.pdf. The costs of responding to corporate data breaches rose from $3.52 million in 2014 to $3.79 million in 2015. *Id.* The study notes that 70% of corporate directors believe board level oversight is paramount. *Id.; see also* Vincent & Higgs, *supra* note 73. Likewise, insurance policies covering losses due to cybersecurity breaches deny coverage when a company fails to meet certain baseline standards. For a discussion of insurance litigation and coverage, see Danielle Gilmore & David Armillei, *The Future Is Now: The First Wave of Cyber Insurance Litigation Commences, and the Groundwork Is Laid for the Coming Storm*, Aspatore, 2016 WL 1089828, at *6 (Feb. 2016).

Although there are several iterations of cyber risk management and IT best practices, the most often cited guidance comes from the National Institute of Standards and Technology (NIST),[78] which recommends that a company's audit committee include a subcommittee dedicated to cyber risk assessment.[79] The majority of the guidance regarding cyber and IT risks in the corporate context focuses on the security levels in place to protect corporate or customer data and the processes in place if a data breach occurs.[80] Common concerns encompass whether employees utilize their own devices[81] or the company's technology, and who has access to these assets.[82] Likewise, the risk associated with ephemeral communications largely depends on whether employees install these applications on personal devices used for work or on corporate devices.[83] IT compliance experts encourage boards to understand how their managers communicate their corporation's IT risks and

---

[78] NIST is a Department of Commerce entity and has recently issued the *Mobile Device Security: Cloud & Hybrid Builds* with collaboration between NIST's National Cybersecurity Center of Excellence and technology industry companies, Microsoft, Intel, Lookout, and Symantec. NAT'L INST. OF STANDARDS AND TECH., NIST SPECIAL PUBLICATION 1800-4B, MOBILE DEVICE SECURITY: CLOUD & HYBRID BUILDS (Nov. 2, 2015) (draft), https://nccoe.nist.gov/projects/building_blocks/mobile_device_security (noting that bring your own device policies expose corporate and sensitive data to attack—for examples calendaring, emails, and contact management—and provides guidance and best practices to avoid these issues).

[79] *See* Davis et al., *supra* note 62, at 630 n.48 (2015). *The Corporate Director's Guidebook* published through the Committee on Corporate Laws of the ABA Section of Business Law. The Institute of Internal Auditors Research Foundation has cautioned directors to ask very specific questions to ensure compliance with their cybersecurity oversight obligations. THE INSTITUTE OF INTERNAL AUDITORS RESEARCH FOUNDATION, CYBERSECURITY: WHAT THE BOARD OF DIRECTORS NEED TO ASK (2014), https://na.theiia.org/special-promotion/PublicDocuments/GRC-Cybersecurity-Research-Report.pdf. Recently, the SEC filed an action under Rule 30(a) of Regulation S-P against Morgan Stanley for failing, as a broker-dealer, to have written policies and procedures reasonably designed to ensure the security and confidentiality of customer information and records. *See* U.S. Sec. Exch. Comm'n, SEC: Morgan Stanley Failed to Safeguard Customer Data, SEC Press Release No. 2016-112 (Jun. 8, 2016), https://www.sec.gov/news/pressrelease/2016-112.html. Although the company had procedures in place, it had not evaluated their procedures' limitations, allowing for an employee to misappropriate customer accounts.

[80] *See generally* Noah G. Susskind, *Cybersecurity Compliance and Risk Management Strategies: What Directors, Officers, and Managers Need to Know*, 11 N.Y.U. J. L. & BUS. 573 (2015); Amanda N. Craig, et al., *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 52(4) AM. BUS. L.J. 721 (2015); Victoria C. Wong, *Cybersecurity, Risk Management, and How Boards Can Effectively Fulfill Their Monitoring Role*, 15 U. C. DAVIS BUS. L.J. 201 (2015).

[81] *See* Steven M. Puiszis, *Can't Live With Them, Can't Live Without Them—Ethical and Risk Management Issues for Law Firms That Adopt a "BYOD" Approach to Mobile Technology*, 2015 PROF. LAW 33, 39–44 (2015) (allowing personal devices for company use is increasing, but issues remain about the security of an individual's device and others' access to it compared to the company's device which may contain higher security protections and encryptions). Successful BYOD policies must address the types of devices that are permitted, the permissible applications, cybersecurity protections, and maintenance. *See* Jonathan Hassell, *7 Tips for Establishing a Successful BYOD Policy*, CIO (May 17, 2012, 8:00 AM), http://www.cio.com/article/2395944/consumer-technology/7-tips-for-establishing-a-successful-byod-policy.html.

[82] *See* Puiszis, *supra* note 81, at 47.

[83] *See generally* Antigone Peyton, *Kill the Dinosaurs, and Other Tips for Achieving Technical Competence in your Law Practice*, 21 RICH. J. L. & TECH. 7 (2015). Ephemeral media

when; what the corporate cybersecurity strategy is; whether management has the appropriate skill set to handle it; how the board evaluates the effectiveness of the cybersecurity efforts; and how the company handles data breach disclosures.[84] Accordingly, failing to inquire about bring your own device policies (BYOD) should be a factor in determining whether a board has met its fiduciary obligations to the shareholders and the public.

Hacking a company's ephemeral media can expose corporate and consumer information.[85] In addition to data breach concerns, the use of ephemeral media to communicate about issues relevant to proper oversight and monitoring of the business potentially exposes the company to fraud and preservation issues.[86] Since April 2014, the SEC Office of Compliance Inspections and Examinations (OCIE) has been monitoring brokerage and ad-

applications cannot control the device itself and whether it has been compromised or whether it has other applications installed on it that are designed to retain information. *See id.*

[84] *See* Glenn Davis, *Prioritizing Cybersecurity: Five Questions for Portfolio Company Boards*, HARV. L. SCH. F. ON CORP. GOVERNANCE & FIN. REG. (May 20, 2016), https://corpgov.law.harvard.edu/2016/05/20/prioritizing-cybersecurity-five-questions-for-portfolio-company-boards/. A recent NASDAQ/Tanium report detailed that, although ahead of the curve, United States directors remain uneducated about risk assessments prior to an attack. *See* Paul Ferrillo, Weil, Gotshal & Manges LLP, *Grading Global Boards of Directors on Cybersecurity*, HARV. L. SCH. F. ON CORP. GOVERNANCE & FIN. REG. (May 1, 2016), https://corpgov.law.harvard.edu/2016/05/01/grading-global-boards-of-directors-on-cybersecurity/.

[85] Initially, users erroneously believed their messages via Snapchat were ephemeral, leading to the Federal Trade Commission's charge of unfair trade practices. *See* Adam R. Pearlman & Erick S. Lee, *National Security, Narcissism, Voyeurism, and Kyllo: How Intelligence Programs and Social Norms Are Affecting the Fourth Amendment*, 2 TEX. A&M L. REV. 719, 789 (2015) (citing Alyssa Newcomb, *Snapchat Settles with FTC Over Claims It Deceived Users About Disappearing Messages*, ABC NEWS (May 8, 2014), http://abcnews.go.com/Technology/snapchat-settles-federal-trade-commission-claims-deceived-users/story?id=23642852); Christina Warren, *Ghost in the Shell, The Snapchat Privacy Illusion*, MASHABLE (Oct. 13, 2014), http://mashable.com/2014/10/13/snapchat-inherently-insecure/ (noting the "inherent security flaw within Snapchat's product: The promise of disappearing images is really just an illusion"). Ultimately Snapchat settled with the government over the false promises that messages would disappear, as well as over misleading statements made about the amount of personal data it collected and its security features. *See* Press Release, Fed. Trade Comm'n, Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False (May 8, 2014), https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were.

[86] *See generally* notes 80 & 83. Additional potential SEC issues include Regulation S-P related to Privacy of Consumer Financial Information under the Gramm-Leach-Bliley Act, requiring financial institutions to notify customers of its privacy policies and the revelation of nonpublic personal information about consumers. The Financial Industry Regulatory Authority (FINRA), a nonprofit self-regulatory agency with oversight responsibility for brokers, dealers and securities firms, conducts enforcement actions where firms fail to address cybersecurity risks and warnings. *See* 17 C.F.R. §162 (2016) (available at https://www.sec.gov/rules/final/2013/34-69359.pdf).

visory firms' cybersecurity practices[87] and continues to list cybersecurity as one of its main investigation topics.[88]

After OCIE's initial sweep in 2014, the SEC investigated R.T. Jones Capital Equities Management, an investment adviser, regarding its failure to create mandatory cybersecurity policies and procedures, resulting in a data breach affecting the private information of 100,000 individuals stored on a third-party server.[89] OCIE and R.T. Jones settled the matter administratively with a censure and a $75,000 penalty.[90] As part of its settlement, the SEC required the company to strengthen its data security systems, appoint an information security manager, notify customers of the data breaches, and provide free identity theft monitoring to those individuals with potentially compromised personally identifiable information.[91]

---

[87] *See generally* OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS, U.S. SEC. AND EXCH. COMM'N, OCIE CYBERSECURITY INITIATIVE, IV.2 NAT'L EXAM PROGRAM RISK ALERT (Apr. 15, 2014), http://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert—Appendix—-4.15.14.pdf. OCIE focused on registered broker-dealers and registered investment advisers and their "cybersecurity governance, identification and assessment of cybersecurity risks, [as well as their] protection of networks and information, risks." *Id.*; *see also* SEC CYBERSECURITY ROUNDTABLE (Mar. 26, 2015), http://www.sec.gov/news/otherwebcasts/2014/cybersecurity-roundtable-032614.shtml; *Cybersecurity Targeted Exam Letter*, FINRA (Jan. 2014), http://www.finra.org/industry/cybersecurity-targeted-exam-letter.

[88] OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS, U.S. SEC. AND EXCH. COMM'N, CYBERSECURITY EXAMINATION SWEEP SUMMARY, IV.4 NAT'L EXAM PROGRAM RISK ALERT (Feb. 3, 2015), http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf. OCIE's focus continues to include risk assessment processes and senior managements' understanding of data use, retention, prevention, and access. *See* OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS, U.S. SEC. AND EXCH. COMM'N, OCIE'S 2015 CYBERSECURITY EXAMINATION INITIATIVE, IV.8 NAT'L EXAM PROGRAM RISK ALERT (Sep. 15, 2015), http://assets.law360news.com/0704000/704173/sec%20risk%20alert.pdf; *see also* Norah C. Avellan, *The Securities and Exchange Commission and the Growing Need for Cybersecurity in Modern Corporate America*, 54 WASHBURN L.J. 193, 226 (2014) (citing DIVISION OF CORPORATE FINANCE, U.S. SEC. AND EXCH. COMM'N, CF DISCLOSURE GUIDANCE: TOPIC NO. 2 (Oct. 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm); Sarah N. Lynch, *SEC on the Prowl for Cyber Security Cases: Official*, REUTERS (Feb. 20, 2015 4:09 EST), http://www.reuters.com/article/us-cyber-idUSKBN0LO28H20150220; DIV. OF INV. MGMT., U.S. SEC. AND EXCH. COMM'N, IM GUIDANCE UPDATE NO. 2015 – 02, CYBERSECURITY GUIDANCE (Apr. 2015), https://www.sec.gov/investment/im-guidance-2015-02.pdf.

[89] R.T. Jones was cited for failure to conduct periodic assessments, lack of firewalls, unencrypted private information on its server, and lack of a data breach plan. R.T. Jones Capital Equities Mgmt., Inc., File No. 3-16827, Investment Advisers Act Release No. 4204 (S.E.C. Sep. 22, 2015), https://www.sec.gov/litigation/admin/2015/ia-4204.pdf.

[90] *Id.*

[91] The SEC need not prove any harm to affected individuals to bring administrative enforcement actions. *See* Peter Sullivan et al., *In Cybersecurity, No Harm Does Not Necessarily Mean No Foul*, LAW360 (Feb. 17, 2016 10:37 AM ET), http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2016_sac/written_materials/5_in_cybersecurity_no_harm_does_not_necessarily_mean_no_foul_law360.authcheckdam.pdf; Report of Investigation Pursuant to Section 21(A) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation to Agency Enforcement Decisions, Exchange Act Release No. 44969, 76 SEC Docket 220 (Oct. 23, 2001), https://www.sec.gov/litigation/investreport/34-44969.htm. *Compare* Chambliss v. CareFirst Inc., No. 15-cv-2288, 2016 WL 3055299 (D. Md. May 27, 2016) (dismissing consumer class action against health insurer for data breach because of lack of actual injury distinguishing *Remijas*' plaintiffs and their injuries), *with* Remijas v. Neiman Marcus Group, LLC, 794 F.3d 668 (7th Cir. 2015) (determining

Issues surrounding ephemeral media are not limited to preventing initial data breaches. Rather, after an attack, preserving evidence from the compromised application is imperative to properly investigate a cyber incident.[92] Without the evidence, investigators are unable to locate "indicators of compromise," which are bits of metadata left by the attacker.[93] A board's failure to identify its data sources and deletion practices interferes with the ability to investigate an attack and creates further claims of potential spoliation discussed below.[94] To resolve these concerns, courts should require boards to assess their cybersecurity risks according to NIST standards, to understand and weigh the risks of internal communication methods, and to implement cybersecurity policies that lessen these risks. If a board fails to carry out these duties, shareholders should have a viable avenue of recourse more substantial than immunizing the board and officers from liability for having a generic policy in place that no one reviews or follows.

III. Federal Intervention into Corporate Oversight Provides Little Shareholder Recourse

As discussed below, there are several federal regulations that facially appear to protect shareholders from corporate mismanagement in the ephemeral media context, but in practice provide minimal private recourse. Distinct from state law fiduciary duties, securities regulations are designed to provide investors with information needed to make an informed investment decision and to deter fraudulent corporate practices.[95] Although shareholders and other private plaintiffs have some legal recourse through securities laws, jurisprudential interpretation of those laws limits relief. In contrast, several federal agencies have jurisdiction in areas relevant to the use of ephemeral

---

plaintiff's had standing to sue even though no evidence of actual identity theft because consumers incurred late charges, the financial loss of buying Neiman Marcus items in lieu of other stores had they known of lax cybersecurity practices, and lost time and money protecting themselves against future identity theft).

[92] Kevin LaCroix, *Guest Post: Ten Cybersecurity Concerns for Every Board of Directors* (Aug. 6, 2015), http://www.dandodiary.com/2015/08/articles/cyber-liability/guest-post-ten-cybersecurity-concerns-for-every-board-of-directors/.

[93] *Id.*

[94] *Id.* (defining best practices for boards of directors from a data preservation and cybersecurity perspective). *See, e.g.*, Cybersecurity Unit, U.S. Dept. of Justice, Best Practices for Victim Responses and Reporting of Cyber Incidents (Apr. 2015), https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_vincidents.pdf.

[95] "[T]here are four categories of required disclosure: first initial disclosure required under the Securities Act [the Securities Act of 1933] when new securities are issued to the public; second, 'periodic reporting,' required under the Exchange Act, which consists of disclosure when securities are registered and then quarterly and annually thereafter; third, proxy disclosure in conjunction with elections at the annual shareholders' meeting; and fourth, disclosure in conjunction with extraordinary corporate events such as a tender offer, merger, or sale of the business."

Cynthia A. Williams, *The Securities and Exchange Commission and Corporate Social Transparency,* 112 Harv. L. Rev. 1197, 1207 (1999).

communications for daily corporate matters and have significant enforcement authority where plaintiff recourse is lacking. Officers, directors, and auditors do not have the protection of the business judgment rule when they willfully violate the federal securities laws as discussed below.[96]

A. Background

Public companies registered under either Section 12 of the Securities Exchange Act of 1934 (the 1934 Act) or the Securities Act of 1933 (the 1933 Act) must file certain disclosure reports with the SEC.[97] Each of the disclosure obligations serves a different purpose at different times in an entity's existence, and entitles investors to information they would find material in making their investment decisions.[98] Nonetheless, existing law does not provide investors with the right to know that (1) a company utilizes ephemeral media as a common form of communication, or (2) that the company might fail to detect red flags in its internal systems because of the use of ephemeral media.[99] Barring a federal disclosure mandate, the national securities exchanges could require the disclosure of ephemeral media use in their listing prerequisites. Further support could be garnered through regula-

---

[96] *See* cases cited *supra* note 74; *see also* Laura Palk, *Ignorance Is Bliss: Should Lack of Personal Benefit Knowledge Immunize Insider Trading?*, 13 BERKELEY BUS. L.J. 101 (2016) (providing a more detailed discussion of the SEC, its powers and enforcement actions, and the prevalence of Second Circuit jurisprudence in securities laws).

[97] *See, e.g.*, Securities Exchange Act of 1934 § 13(a), 15 U.S.C. § 78m(a) (2016); *see also* U.S. SEC. AND EXCH. COMM'N, SMALL BUSINESS AND THE SEC (Oct. 10, 2013), https://www.sec.gov/info/smallbus/qasbsec.htm; U.S. SEC. AND EXCH. COMM'N, THE LAWS THAT GOVERN THE SECURITIES INDUSTRY (Oct. 1, 2013), https://www.sec.gov/about/laws.shtml. Publicly held companies are (a) those companies traded on a national securities exchange, for example, the New York Stock Exchange (NYSE); and (b) those with 500 or more shareholders and $10 million or more in assets. 15 U.S.C. § 78l(g) (2015) (defining public companies); *see also* 17 C.F.R. § 240.12g-1 (2016) (noting exempted companies). Under the Jumpstart Our Business Startups Act of 2012 (JOBS Act), Pub. L. No. 112-106, 126 Stat. 306, companies with under $1 billion in annual revenue are exempt from certain onerous SEC and federal regulations for five years after they go public. *Id.* §§ 101, 102 (codified as amended at 15 U.S.C. § 77b(a)(19) (2016) and scattered sections of 15 U.S.C.). Stock markets and exchanges are separate from the SEC and are self-regulatory organizations. To trade on the NYSE or the NASDAQ Stock Market (NASDAQ), companies may be required to comply with rules that do not otherwise exist. *See* Harold S. Bloomenthal & Samuel Wolff, *Securities and Federal Corporate Law, Securities Markets and Broker-Dealer Regulation*, 3D SEC. & FED. CORP. LAW § 23:125 (2d ed.) (2016).

[98] *See* TSC Industries, Inc. v. Northway, Inc., 426 U.S. 438, 445 (1976) (discussing materiality as the threshold for securities laws and their goals).

[99] Congressman Jim McDermott (D-Wash.) has proposed amendments to the mandatory reporting requirements of SOX to include disclosures of cyber-security systems, associated risks, and whether an IT expert is on the audit committee. *See* The Cyber-security Systems and Risks Reporting Act, H.R. 5069, 114th Congress (Apr. 26, 2016), https://www.congress.gov/bill/114th-congress/house-bill/5069. A less exacting measure has been introduced in the Senate by Sens. Jack Reed (D-R.I.) and Susan Collins (R-Maine) under the Cybersecurity Disclosure Act of 2015. *See* Cybersecurity Disclosure Act of 2015, S. 2410, 114th Congress (Dec. 17, 2015).

tion, thereby reducing the ill effects the use of ephemeral communications may inflict.

After the financial scandals of Enron and WorldCom among others, Congress successfully amended corporate governance and disclosure laws through the passage of the Sarbanes-Oxley Act of 2002 (SOX).[100] SOX provides a bar that the exchanges and SEC monitor for listed companies.[101] In addition to the disclosure obligations of SOX, companies now have requirements regarding record keeping, internal accounting controls, and chief executive officers' or chief financial officers' certifications regarding proper disclosures in financial statements.[102] Although SOX did not mandate it, the SEC recommends that companies maintain disclosure committees to ensure compliance with their SOX obligations.[103] These disclosure committees are designed to establish internal policies and procedures to ensure the relevant officers have the information they need to make proper SEC disclosures and risk assessments.[104] As part of this new regulatory scheme, external auditors registered through the Public Company Accounting Oversight Board (PCAOB) must ensure corporate management's compliance with SOX.[105] In particular, SOX requires corporate management to evaluate the company's

---

[100] *See* Sarbanes-Oxley Act of 2002 (SOX), Pub. L. No. 107-204, 116 Stat. 745 (codified as amended in various sections of 15 U.S.C. and 18 U.S.C., for example 15 U.S.C. § 7201 (2016)). Title I of SOX created the Public Company Accounting Oversight Board, a nonprofit organization charged with registering and inspecting public accounting firms, and promulgating auditing standards. Title II of SOX defines the roles of auditors and their independence from the companies they audit. Title III of SOX regulates corporate governance, creates corporate audit committees and penalties for officers and directors if they violate SOX. Title IV of SOX discusses the increase in disclosure requirements. Titles V-IX of SOX address conflicts of interests and associated penalties. *See* James J. Park, *Two Trends in the Regulation of the Public Corporation*, 7 Ohio St. Entrep. Bus. L. J. 429, 432 (2012).

[101] *See, e.g.*, SOX § 301 (amending Section 10A of the Exchange Act, 15 U.S.C.A. § 78j-1 by adding subsection (m)).

[102] *Id.*; *see also id.* § 404 (codified as amended at 15 U.S.C. § 7262(a)(1) (2016)) (internal controls); *id.* § 906 (codified as amended at 18 U.S.C. § 1350 (2016)) (financial statements).

[103] *See* Certification of Disclosure in Companies' Quarterly and Annual Reports, Exchange Act Release No. 33-8124, 78 S.E.C. Docket 875 (Aug. 28, 2002) (indicating that to comply with SOX obligations, companies need policies and procedures in place through a designated committee designed to capture relevant financial and nonfinancial information for disclosure).

[104] Larry D. Thompson, *The Responsible Corporation: Its Historical Roots and Continuing Promise*, 29 Notre Dame J.L. Ethics & Pub. Pol'y 199, 266 n.139 (2015).

[105] SOX §§ 101–09 (codified as amended at 15 U.S.C § 7211–19 (2016)) (relating to the establishment and powers of the PCAOB). Both internal audit committees and external auditors must ensure proper internal corporate controls designed to detect and prevent material misstatements in financial statements. 15 U.S.C. § 78m(b)(2)(A)–(B) (2016); 17 C.F.R. §§ 240.13a-15(a), 15(d)–(f) (2016). SOX mandated companies to create internal audit committees, and required companies' chief executive officer and external auditor to certify the accuracy of the company's financial statements and internal controls. SOX § 302(a) (codified as amended at 15 U.S.C. § 7241(a) (2016)). Although one might argue that ephemeral media will not be used to discuss information related to financial statement disclosure requirements, auditors consider, in a more general sense, whether the internal control allows proper management oversight, and the prevention or detection of fraud. *See I8: Management Internal Control Reports Over Financial Reporting*, WGL Handbook SEC Acct. & Disclos. 18 (2016). If most communication and decision-making occurs through transitory means, without a record of the transactions or the details of the decision-making process, the auditor will have minimal infor-

internal control system annually and to report the system's effectiveness to the company's audit committee and to external auditors.[106] One identifiable risk of using ephemeral media is the "unauthorized access to data that might result in destruction of data or improper changes to data . . . ."[107] The daily use of ephemeral media among employees or management could heighten the risk of material misrepresentations in corporate financial statements, thereby subjecting the officers, directors, and auditors to legal liability.[108]

B. Private Actions

Although SOX obligations do not create breach of fiduciary duty claims for shareholder-plaintiffs,[109] there are a variety of SEC provisions designed to ensure that disclosures do not contain material misstatements or omissions. Whether shareholder-plaintiffs may recover for the failure to disclose in SEC filings depends on which section of the SEC rules a plaintiff pursues.[110] Compared to the SEC, individual plaintiffs face a more difficult procedural and legal challenge in bringing a private claim against a corporation, its officers, directors, and auditors discussed below.

Unlike SEC enforcement actions, a private suit must comply with the heightened pleading standards of the Private Securities Litigation Reform

---

mation upon which to base his decision, affecting his ability to determine the integrity and reliability of the information through a test sample.

[106] *See* SOX § 404 (codified as amended at 15 U.S.C. § 7262 (2016)). The auditor must attest to, and report on, management's own assessment of its internal controls and effectiveness. *See* SOX § 103(a)(2)(A)(iii) (codified as amended at 15 U.S.C. § 7213(a)(2)(A)(iii) (2016)); *see also* AUDITING STANDARD § 2201 (PUB. CO. ACCT. OVERSIGHT BD. 2016), https://pcaobus.org/Standards/Auditing/Pages/AS2201.aspx. The company's audit committee has ultimate oversight of the financial reporting, internal controls, the internal audit, and engaging the external independent auditors. *See* SOX § 301 (codified as amended at 15 U.S.C. § 78j–1(m) (2016)). The audit committee must determine whether a "material weakness" might exist in an area relevant to the company's existing or future financial health. *See* 17 C.F.R. § 229.601(b)(31)(i)(5)(a) (2016).

[107] AUDITING STANDARD § 2110-B4 (PUB. CO. ACCT. OVERSIGHT BD. 2016); *see also* Public Company Accounting Oversight Board; Notice of Filing of Proposed Rules on Auditing Standards, Exchange Act Release No. 62,919, 75 Fed. Reg. 59331 (Sept. 15, 2010). The overarching concern for external auditors is the integrity and reliability of management's records, ensuring no misstatements on its financial statements. *See* W. R. Koprowiski et al., *Financial Statement Reporting of Pending Litigation: Attorneys, Auditors, and Differences of Opinions*, 15 FORDHAM J. CORP. & FIN. L. 439, 440–41, 45 nn.35–47 (2010) (discussing auditors' obligations to express whether a financial statement is reliable based on an examination of the company's books and records under former Auditing Standard 12 and the guidance of the Generally Accepted Accounting Principles issued by the Financial Accounting Standards Board).

[108] *See also* Thad A. Davis et al., *supra* note 62, at 649. *See generally* AUDITING STANDARD § 2110-B4 (PUB. CO. ACCT. OVERSIGHT BD. 2016).

[109] *See* Byron F. Egan, *Fiduciary Duties of Corporate Directors and Officers in Texas*, 43-SPG TEX. J. BUS. L. 45, 96–97 (2009). *But see* Eric L. Talley, *Corporate Inversions and the Unbundling of Regulatory Competition*, 101 VA. L. REV. 1649, 1696 (2015) (detailing recent cases stating that federal fiduciary duty arguments under SOX and the Dodd Frank Wall Street Reform and Consumer Protection Act of 2010 would likely fail).

[110] *See* Michael Evans, *Adding A Due Diligence Defense to § 13(b) and Rule 13b2–2 of the Securities Exchange Act of 1934*, 72 WASH. & LEE L. REV. 901, 914 (2015) (discussing the distinctions between three securities provisions related to disclosures).

Act (PLSA) and Federal Rules of Civil Procedure Rule 9(b) by "stating with particularity the circumstances constituting fraud."[111] The potential relevant derivative claims against officers, directors, or auditors for the corporate use of ephemeral media include (1) fraudulent misstatements or omissions in connection with a sale of securities under Rule 10b-5;[112] and (2) material misleading statements or omissions in the registration statement under section 11 of the 1933 Act.[113] Each of these sections has its own limitations. The most challenging aspect of a Rule 10b-5 claim is proving the necessary "strong inference of scienter" to establish fraud.[114] Under section 11, although a defendant is liable regardless of his intent, section 11 claims are limited to five classes of individuals, and the plaintiffs must demonstrate their purchase relates specifically to the material misstatement or omission.[115]

Regarding both a Rule 10b-5 and a section 11 claim, a plaintiff must demonstrate the statement or omission was material.[116] Moreover, with respect to misstatements in disclosures, a plaintiff must establish that the statements were false and misleading, including specifically "why and how that is so."[117] An added requirement for a claim of a material misstatement under Rule 10b-5 is that the complaint must "(1) specify the statements that the plaintiff contends were fraudulent, (2) identify the speaker, (3) state where

---

[111] *See In re* MF Glob. Holdings Ltd. Sec. Litig., 982 F. Supp. 2d 277, 303 (S.D.N.Y. 2013). With respect to claims under § 11 of the 1934 Act discussed herein, no heightened pleading is required if the allegations do not involve fraud; however, many times § 11 claims are plead alongside fraud claims. *See, e.g.*, *In re* Citigroup Inc. Bond Litigation, 723 F. Supp. 2d 568, 586 (S.D.N.Y. 2010) (non-fraudulent § 11 liability claims can assert ordinary negligence).

[112] 17 C.F.R. § 240.10b-5 (2016) (prohibition includes the fraudulent omission or statement of material fact in disclosures). Private plaintiffs bear a significant burden in establishing the elements of a 10b-5 fraud claim and are rarely successful. *See* Evans, *supra* note 110, at 913; *see also* Ganino v. Citizens Utils. Co., 228 F.3d 154, 161 (2d Cir. 2000) (detailing the elements of a Rule 10b-5 claim).

[113] 15 U.S.C. § 77k (2012) (prohibiting materially misleading statement or omissions in registration statements). Liability under Section 11 is limited to five classes of defendants and plaintiffs must connect their purchases to the fraudulent statement. *See* Evans, *supra* note 110, at 914.

[114] *See* Evans, *supra* note 110, at 912–13; *see also In re* Lions Gate Entertainment Corp. Sec. Litig., 165 F. Supp. 3d 1, 11 (S.D.N.Y. 2016) (finding no duty to disclose a pending SEC investigation and lack of an inference of the level of scienter required for Rule 10b-5 liability).

[115] 15 U.S.C. § 77k(a)(1)–(5) (2016). Thus, not all current officers and directors would necessarily be liable if they either did not sign it, did not prepare it, or were not yet a director of the company at the time of the statement. 15 U.S.C. § 77k(a)(4) (2016); *see In re* Glob. Crossing, Ltd. Sec. Litig., 313 F. Supp. 2d 189, 195 (S.D.N.Y. 2003).

[116] *See, e.g.*, TSC Industries, Inc. v. Northway, Inc., 426 U.S. 438 (1976).

[117] *See* Carpenters Pension Trust Fund of St. Louis v. Barclays PLC, 750 F.3d 227, 236 (2d Cir. 2014) (quoting Rombach v. Chang, 355 F.3d 164, 174 (2d Cir. 2004)). "Rule 10b-5 imposes no duty to disclose all material, nonpublic information, once a party chooses to speak, it has a duty to be both accurate and complete." *In re* MF Glob. Holdings Ltd. Sec. Litig., 982 F. Supp. 2d 277, 303 (S.D.N.Y. 2013) (quoting Plumbers' Union Local No. 12 Pension Fund v. Swiss Reinsurance Co., 753 F. Supp. 2d 166, 180 (S.D.N.Y. 2010)); *see also* Donald C. Langevoort, G. Mitu Gulati, *The Muddled Duty to Disclose Under Rule 10b-5*, 57 VAND. L. REV. 1639, 1664 (2004) (discussing the duty to disclose and the effect of certain omissions).

and when the statements were made, and (4) explain why the statements were fraudulent."[118] Whereas, an omission of fact is actionable only if the defendant has a duty to disclose those omitted facts or the omission of the facts renders the disclosure misleading.[119] Whether the plaintiff must allege facts that a specific individual acting on behalf of the corporation made the misleading statement with the requisite state of mind, or whether pleading a "collective" or "corporate" scienter[120] is sufficient is the subject of circuit debate.[121]

Defendants may defend an action alleging misleading information or omissions in company disclosures by arguing that they exercised due diligence.[122] The viability of this defense depends on who the defendants are, and what red flags existed at the time of the misstatement.[123] Senior level officers and even directors face a presumption that their positions alone render it unlikely they were unaware of the misstatements.[124] Arguably, officers and directors who know—or could know through simple inquiry—that corporate employees regularly use ephemeral media to discuss corporate matters must determine whether adequate controls are in place to prevent

---

[118] *See* Romach v. Chang, 355 F.3d 164, 170 (2d Cir. 2004) (quoting Mills v. Polar Molecular Corp., 12 F.3d 1170, 1175 (2d Cir. 1993)*; see also* 15 U.S.C. § 78u-4(b)(1) (2016). "At the pleading stage, a plaintiff satisfies the materiality requirement of Rule 10b-5 by alleging a statement or omission that a reasonable investor would have considered significant in making investment decisions." Caiola v. Citibank, N.A., New York, 295 F.3d 312, 329 (2d Cir. 2002).

[119] *In re* Bank of Am. AIG Disclosure Sec. Litig., 980 F. Supp. 2d 564, 575 (S.D.N.Y. 2013), *aff'd*, 566 F. App'x 93 (2d Cir. 2014). Such a duty arises either by specific legal obligation or in connection with an ongoing duty to ensure that existing statements are not rendered misleading by failing to disclose the additional information. *Id.*

[120] Collective or corporate scienter "create a strong inference that someone whose intent could be imputed to the corporation acted with the requisite scienter." Teamsters Local 445 Freight Div. Pension Fund v. Dynex Capital, 531 F.3d 190, 195 (2d Cir. 2008).

[121] *Compare* Southland Sec. Corp. v. INSpire Ins. Solutions, Inc., 365 F.3d 353, 366–67 (5th Cir. 2004) (finding at least one defendant acting on behalf of the company must be implicated) *with* the idea that alleging collective scienter is permissible, but plaintiffs must still meet heightened and difficult pleading standards. *See, e.g.*, Teamsters Local 445 Freight Div. Pension Fund, 531 F.3d at 195; Makor Issues & Rights, Ltd. v. Tellabs, Inc., 513 F.3d 702, 710 (7th Cir. 2008); Glazer Capital Mgmt., LP v. Magistri, 549 F.3d 736, 744 (9th Cir. 2008); City of Monroe Employees Retirement Syst. v. Bridgestone Corp., 399 F.3d 651, 684, 689–90 (6th Cir. 2005).

[122] The due diligence defense is the reasonable reliance on expert opinions or the reasonable investigation into the accuracy of the records. For example, where a non-expert defendant, other than the issuer, reasonably relies on an expert's opinion related to an "expertised" portion of a registration statement, or if the defendant, expert or non-expert, makes a reasonable investigation into the accuracy of the registration statement, then the defense is satisfied. *See* Evans, *supra* note 110, at 933 (citing 15 U.S.C. § 77k (1998)); *see also* 15 U.S.C. §77k(b)(3) (2016) (distinguishing between expertised and non-expertised portions of the registration statement and between experts and non-experts).

[123] *See* Evans, *supra* note 110, at 935 (citing Escott v. BarChris Constr. Corp., 283 F. Supp. 643, 652 (S.D.N.Y. 1968) and *In re* WorldCom, Inc. Sec. Litig., 346 F. Supp. 2d 628, 634 (S.D.N.Y. 2004)); *see also In re* WorldCom, 346 F. Supp. 2d at 634 (ignoring red flags negates the defense of a reasonable investigation).

[124] *See* Evans, *supra* note 110, at 935.

corporate misconduct and to detect other red flags for full and proper disclosure in required SEC filings.

Even where a shareholder-plaintiff believes the nondisclosure was fraudulent, his ability to successfully sue for an omission is severely constrained. In *Omnicare, Inc. v. Laborers District Council Construction Industry Pension Fund*,[125] investors sought relief as a class against Omnicare, Inc. and its officers and directors for material misstatements and omissions in its registration statement under section 11 of the Securities Act of 1933.[126] The plaintiffs claimed the company's statement regarding its compliance was a material misstatement and omission because the officers and directors knew they were at a heightened risk of violating federal anti-kickback laws.[127] If the statement of opinion omits facts that are needed to ensure the veracity of the issuer's statements, the issuer must assess whether the omitted facts render the opinion misleading to a reasonable investor.[128] The Supreme Court determined, by analyzing the statements in the context of misrepresentation tort theory, that the omission in *Omnicare* was material because the company claimed to have superior knowledge of the facts, and yet failed to disclose the negative legal opinion it had received about its lack of legal compliance.[129]

Like claims against directors, and as evidenced by the *Omnicare* case, private plaintiffs can sue accountants for either section 11 or Rule 10b-5 claims.[130] To hold an auditor, internal or external, liable under section 10(b),[131] a plaintiff must prove that the auditor had an intent to deceive,

---

[125] 135 S. Ct. 1318 (2015).

[126] *See* 15 U.S.C. § 77k(a) (2016) (providing a private right of action for material misstatements or omissions in a registration statement).

[127] *Omnicare, Inc.*, 135 S. Ct. at 1324.

[128] *Id.*

[129] *Id.* at 1329. The Supreme Court ultimately remanded the case to the lower court for consideration of these factors. *Id.* at 1333.

[130] Unlike a Rule 10b-5 claim, Section 11 of the 1933 Act liability simply requires the accountant to contribute to the registration statement that included a material misstatement or omission and investors purchased the security under that registration statement. *See In re* Stac Elecs. Sec. Litig., 89 F.3d 1399, 1403–04 (9th Cir. 1996) (citing Herman & MacLean v. Huddleston, 459 U.S. 375, 382 (1983)) (indicating that no scienter is required for Section 11 liability only that the omission or misstatement in the registration statement was material and would have mislead a reasonable investor); *cf. In re* Initial Public Offering Sec. Litig., 241 F. Supp. 2d 281, 325 (S.D.N.Y. 2003) (clarifying that Federal Rules of Civil Procedure Rule 9(b) requires a plaintiff to plead with particularity those facts establishing fraud for securities violations, but only where fraud is an essential element of the claim and that Rule 9(b) does not apply to *all* allegations of a Section 11 claim); 15 U.S.C. § 77k (2012).

[131] Under Section 10(b) (codified at 15 U.S.C. § 78j(b) (2016)) and Rule 10b-5, a private plaintiff must prove: "(1) a material misrepresentation or omission by the defendant; (2) scienter; (3) a connection between the misrepresentation or omission and the purchase or sale of a security; (4) reliance upon the misrepresentation or omission; (5) economic loss; and (6) loss causation." *See* Halliburton Co. v. Erica P. John Fund, Inc., 134 S. Ct. 2398, 2407 (2014) (quoting Amgen Inc. v. Connecticut Retirement Plans and Trust Funds, 133 S. Ct. 1184, 185 (2013)). A Section 10(b) violation includes a prohibition on market manipulation through false or misleading statements or omissions. *See In re* MF Glob. Holdings Ltd. Sec. Litig., 982 F. Supp. 2d 277, 303 (S.D.N.Y. 2013).

manipulate, or defraud the shareholder, demonstrated by behavior that is "highly unreasonable and which represents an extreme departure from the standards of ordinary care."[132] Examples of behavior sufficient to establish recklessness include those instances where a defendant has specific evidence contradicting the disclosed public statements or where the defendants "failed to review or check information that they had a duty to monitor, or ignored obvious signs of fraud."[133] Thus, individual liability for officers, directors, and auditors is unlikely where there is no underlying duty to comply with cybersecurity best practices and no duty to specifically inquire about the methods of daily corporate communications and the risks posed by those methods.

Proving the requisite scienter against any defendant is a difficult task. For example, the Southern District of New York found that an outside auditor was not liable for securities violations even though the auditor noticed risks of fraud and weaknesses in the company's internal controls which the company had previously ignored.[134] The court found that even if the auditor had performed a better audit, the only result would have been earlier detection of fraud.[135] The evidence indicated that the company tricked the auditor, not that the auditor's recklessness enabled the fraud.[136] It is not "enough to 'merely alleg[e] that the auditor had access to the information by which it could have discovered the fraud . . . .'"[137] To succeed, a plaintiff must demonstrate the auditor ignored red flags that would be sufficient evidence of *actual* fraud.[138]

In light of existing jurisprudence, an auditor, and an officer or director by analogy, will not be liable for failing to inquire about corporate commu-

---

[132] *See MF Glob. Holdings*, 982 F. Supp. 2d at 305.

[133] *Id.*

[134] *See In re* Longtop Fin. Techs. Ltd. Sec. Litig., 939 F. Supp. 2d 360, 391 (S.D.N.Y. 2013) (dismissing derivative claims against external auditor under § 10(b) as there was no requisite scienter for fraud and the failure to disclose the red flags did not amount to a material misstatement).

[135] *Id.*

[136] *Id.*; *see also* Stephenson v. Citco Group Ltd., 700 F. Supp. 2d 599, 622 (S.D.N.Y. 2010) (discussing the varied court rulings on when red flags are sufficient to warrant scienter and liability), *rev'd on other grounds*, 482 Fed. Appx. 618 (2d Cir. 2012).

[137] *See* Stephenson v. Pricewaterhousecoopers, LLP, 768 F. Supp. 2d 562, 573 (S.D.N.Y. 2011) (alterations in original) (quoting *In re* Tremont Sec. Law, State Law & Ins. Litig., 703 F. Supp. 2d 362, 370 (S.D.N.Y. 2010)).

[138] *See* Iowa Public Employee's Retirement System v. Deloitte & Touch LLP, 973 F. Supp. 2d 321, 465 (S.D.N.Y. 2013) (holding that there is no Rule 10b–5 liability even if an auditor fails to investigate certain red flags that could have uncovered fraud), *aff'd*, 558 Fed. App'x 138 (2d Cir. 2014); *see also In re* Advanced Battery Techs., 781 F.3d 638, 646 (2d Cir. 2015) (finding even a lack of due diligence is insufficient to establish the requisite scienter). Use of ephemeral forms of communication cannot only implicate SOX internal control and disclosure obligations, but where the communication is designed to circumvent internal controls, liability may attach under Section 13(b)(5). *See* 15 U.S.C. § 78m(b)(5) (2010) ("no person shall knowingly circumvent or knowingly fail to implement a system of internal accounting controls or knowingly falsify any book, record, or account . . . ."). Similar to other claims of securities fraud, a private plaintiff must demonstrate scienter. *See* SEC v. Retail Pro, Inc., 673 F. Supp. 2d 1108, 1141 (S.D. Cal. 2009).

nication methods. This decreases the likelihood of discovering employee misconduct such as insider trading, bribery of foreign officials, or financial fraud, potentially exposing the company to substantial financial loss. A shareholder-plaintiff has no recourse unless he can prove that the auditor actually knew the misconduct was occurring or knew that ephemeral media was used to hide the misconduct. Because there is such a high bar for success in a private action, administrative enforcement claims are currently the only mechanism through which officers, directors, and auditors can be held accountable for such clear negligence.

C. Administrative Enforcement

Although shareholders are limited in their ability to bring derivative claims, the SEC can initiate administrative actions for failing to properly monitor internal controls.[139] In the context of ephemeral communications, the SEC can enforce section 13 of the 1934 Act against companies that provide false or misleading information to an accountant or in public disclosure documents.[140] SEC enforcement liability attaches when an officer or a director, either "directly or indirectly, makes or causes to be made a materially false or misleading statement or omission to an accountant in connection with an audit or the preparation or filing of SEC required documents."[141] Whether a defendant's lack of scienter and due diligence defense protects a defendant from section 13(b) liability is the subject of a circuit court split.[142] Moreover, in section 13(b) claims, immaterial statements that reflect an un-

---

[139] *See* Gerry Pecht, Peter Stokes, Mark Oakes, *SEC Targets Companies, Executives, Directors, and Outside Accountants over Deficiencies in Internal Controls,* SEC COMPLIANCE BEST PRACTICES, 2016 WL 1595379, at *3 (2016).

[140] 17 C.F.R. § 240.13b2-2a (2016). Additionally, with respect to other disclosure obligations, the SEC enforces Rule 12b-20, *see* 17 C.F.R. § 240.12b-20 (2016), although there is no private right of action for either, *see In re* Anika Therapeutics, Inc., File No. 3-11006, Exchange Act Release No. 47167 (S.E.C. Jan. 13, 2003).

[141] *Id.*; *see, e.g.*, U.S. Sec. Exch. Comm'n., Ernst & Young to Pay $11.8 Million for Audit Failures, SEC Press Release No. 2016-219 (Oct. 18, 2016), https://www.sec.gov/news/press-release/2016-219.html (announcing a penalty against Ernst & Young for failing to detect fraud in four years' worth of audits by relying on unsubstantiated explanations from the corporate officers and directors available); U.S. Sec. Exch. Comm'n, Monsanto Paying $80 Million Penalty for Accounting Violations, SEC Press Release No. 2016-25 (Feb. 9, 2016), https://www.sec.gov/news/pressrelease/2016-25.html (Monsanto settled an SEC books and records violation that it had insufficient internal accounting controls to properly account for millions of dollars in rebates and failed to properly recognize expenses in financial statements; the chief executive officer and chief financial officer had not engaged in misconduct, but reimbursed the company for cash and stock awards during the time period as required under SOX.); U.S. Sec. Exch. Comm'n, SEC Charges Biopesticide Company and Former Executive with Accounting Fraud, SEC Press Release No. 2016-32 (Feb. 17, 2016), https://www.sec.gov/news/press-release/2016-32.html (finding a violation of the SEC books and records provisions that the chief operating officer concealed information from the finance personnel and independent auditor; the chief executive officer and the chief financial officer, despite no finding of misconduct, reimbursed the company for incentive-based compensation for the time period pursuant to SOX obligations).

[142] *See* Evans, *supra* note 110, at 923–29.

reasonable inaccuracy in the corporation's books, records, or reports can support SEC enforcement actions.[143] Moreover, Section 13(b) provides no private right of action.

In the ephemeral media context, the SEC enforcement efforts focus on officers' and directors' lack of documentary evidence of the adequacy of their corporate internal controls.[144] Directors must ensure they have sufficient documentation to support their conclusions and may not rely solely on outside advisors for their assessments.[145] However, if companies lack policies and

---

[143] *See* Evans, *supra* note 110, at 919 ("Thus, unimportant misrepresentations are not fraudulent under Rule 10b-5, and inconsequential omissions in a registration statement do not establish § 11 liability. But § 13(b) is qualified by a standard of reasonableness. Consequently, § 13(b) reaches unreasonable inaccuracy in corporate records even if these inaccuracies are nonmaterial."). The question of reasonableness is addressed in SEC Rule 176, 17 C.F.R. § 230.176 (2016); *see also* 15 U.S.C. § 78m(b)(2)(A) (2016) (companies must keep books and records accurate to a reasonable detail).

[144] 17 C.F.R. § 229.308 (2016) (requiring that under Item 308 of Regulation S-K, management "must maintain evidential matter, including documentation, to provide reasonable support for management's assessment of the effectiveness of the registrant's internal control over financial reporting."); *see also* Commission Guidance Regarding Management's Report on Internal Control, Exchange Act Release No. 33-8810 (June 27, 2007), https://www.sec.gov/rules/interp/2007/33-8810.pdf ("Management is responsible for maintaining evidential matter, including documentation, to provide reasonable support for its assessment."). Further, the Internal Control-Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO Framework) provides that management should "develop and retain documentation to support the statements made." *See* Pecht et al., *supra* note 139, at *4. Despite the difficulty in bringing a private claim, the SEC has increased its number of administrative enforcement actions against accountants and auditors for misstatements of opinion. *See In re* Magnum Hunter Res. Co., File No. 3-17166, Exchange Act Release No. 77345 (S.E.C. March 10, 2016), https://www.sec.gov/litigation/admin/2016/34-77345.pdf (SEC charged the company and its chief financial officer, chief accounting officer, and outside auditing consultants for identifying internal control deficiencies they found would lead to material weaknesses in financial reporting and yet failed to attempt to resolve the issues); Pecht, *supra* note 139, at *1–3. Moreover, the SEC's initiative seeks enforcement and compliance through the "broken window" policy designed to capture internal control failures even where no allegations of fraud are present. Linda L. Griggs, Peter K.M. Chan, *The SEC's Accounting and Internal Control Cases Are Expected to Increase as a Result of its Financial Reporting and Audit Task Force*, Business Law Today, Oct. 2015, http://www.americanbar.org/publications/blt/2015/10/04_griggs.html.

[145] *See* Pecht et al., *supra* note 139, at *3 (discussing recent SEC administrative enforcement actions under the books and records requirements of SEC Sections 13(a), 13(b)(2)(A) and 13(b)(2)(B) and Rules 12b-20, 13a-1, 13a-11, and 13a-13, including against the chief executive officer and the chief financial officer of QSGI Inc. for claiming to have reviewed internal controls under the COSO Framework and yet being completely unfamiliar with its guidelines); *see also In re* Marc Sherman, File No. 3-15992, Exchange Act Release No. 74765, 2015 WL 1776221 (S.E.C. Apr. 20, 2015) (SEC imposing sanctions against Mr. Sherman for violations of Rule 10b-5 for false certifications under SOX) (S.E.C. July 30 2014); *In re* Edward L. Cummings, CPA, File No. 3-15991, Exchange Act Release No. 72722 (S.E.C. July 30, 2014)); *In re* Saba Software, Inc., File No. 3-16161, Exchange Act Release No. 73202, 2014 WL 4726473 (S.E.C. Sept. 24, 2014) and Exchange Act Release No. 74300, 2015 WL 692237 (S.E.C. Feb. 19, 2015) (requiring chief executive officer to reimburse the company for bonuses and profits because he lacked documentary evidence regarding internal control reviews even though no misconduct shown). Moreover, where a director falsely claimed reimbursement expenses, the SEC imposed a $750,000 penalty on the company for failing to have sufficient controls designed to detect the underreporting of executive compensations. *See In re* Polycom, Inc., File No. 3-16464, Exchange Act Release No. 2015-74613 (S.E.C. Mar. 31, 2015). Addi-

procedures dedicated to the use of ephemeral media, it will be difficult for officers and directors to demonstrate that adequate internal controls actually exist.[146] The very nature of the ephemeral media eliminates signs of red flags.[147] Knowing that one's corporation utilizes this method of communication is tantamount to a conscious disregard of any misconduct.[148] Nonetheless, while the SEC may seek administrative enforcement for these discrepancies, shareholder-plaintiffs are deprived of success in the courts.[149] Implementation of a regulatory affirmative duty to disclose the use of ephemeral corporate communications along with corporate appropriate use policies would enhance shareholders' ability to bring private rights of actions.

D. Nonfinancial Disclosures as a Basis for Managerial Liability

The initial question regarding the use of ephemeral communication is whether knowledge of the use alone warrants disclosure. Arguably, it does not. However, the nature of the discussions[150] or the nature of the business[151]

---

tionally, the SEC imposed a $1.5 million penalty against Home Loan Servicing Solutions, Ltd. for failing to maintain written policies and procedures requiring recusal of its chairman in related party transactions because the chairman ultimately approved certain transactions in violation of the "policy" against it. *See In re* Home Loan Servicing Solutions Ltd., File No. 3-16882, Exchange Act Release No. 76074 (S.E.C. Oct. 5, 2015).

[146] *See, e.g.*, Abrams v. Baker Hughes Inc., 292 F.3d 424, 432 (5th Cir. 2002) (finding the "mere publication of inaccurate accounting figures or failure to comply with generally accepted accounting principles, without more, does not establish scienter"); Plumbers and Pipefitters Local Union No. 719 Pension Trust Fund v. Conseco Inc., Civ. No. 09-6966, 2011 WL 1198712, at *22 (S.D.N.Y. 2011) ("A failure 'to identify problems with the defendant-company's internal controls and accounting practices does not constitute reckless conduct sufficient for § 10(b) liability.'" (quoting Novak v. Kasaks, 216 F.3d 300, 309 (2d Cir. 2000))). However, where there is evidence the officers knew of the severity of control deficiencies and did nothing about it, a claim may arise. *See, e.g.*, Varghese v. China Shenghuo Pharmaceutical Holdings, Inc., 672 F. Supp. 2d 596, 602–03, 610–11 (S.D.N.Y. 2009) (finding sufficient allegations to survive a motion to dismiss where plaintiffs alleged defendants knew the company had no internal control improvement procedures in place and yet publicly stated that efforts were in place); *In re* Barrick Gold Sec. Litig., 2015 WL 1514597 (S.D.N.Y. 2015), recons. denied, 2015 WL 3486045 (S.D.N.Y. 2015) (finding sufficient allegations of public misstatements as defendants had contradictory information concerning their environmental approval disclosures).

[147] *See* Davis et al., *supra* note 62 at 637, 649; *see also In re* Walt Disney Co. Derivative Litig., 906 A.2d 27, 53 (Del. 2006) (finding duty to be informed).

[148] *See* Hayes v. Gross, 982 F.2d 104, 106–07 (3d Cir. 1992). *But see* Ades v. Deloitte & Touche, 799 F. Supp. 1493, 1499 (S.D.N.Y. 1992) (inference of recklessness may be drawn from facts demonstrating that defendants disseminated material knowing that its method of preparation was so lacking as to render dissemination of the material reckless).

[149] Directors owe a corresponding duty to disclose material information; however, to be found liable for a breach of fiduciary duty for such failure, the directors must "deliberately misinform shareholders about the business of the corporation either directly or by a public statement." *In re* Citigroup Inc. S'holder Derivative Litig., 964 A.2d 106, 132 (Del. Ch. 2009); *see also* Tow v. Bulmahn, Civ. No. 15-3141, 2016 WL 1722246 (E.D. La. April 29, 2016) (explaining that knowledge of inadequate internal controls which could lead to materially harmful behavior was insufficient to establish a conscious disregard of fiduciary duty). SEC enforcement may be the only solution. *See* Kerr, *supra* note 25; Butler, *supra* note 25.

[150] For example, discussing bribery payments.

can dictate whether disclosure is warranted when corporate officers or employees delete communications that might evidence criminal wrongdoing,[152] or might destroy evidence.

There are two basic types of disclosure, mandatory and voluntary; further categorized as either financial or nonfinancial. Information related to a company's financial statements necessary to ensure there are no material misstatements must be disclosed.[153] Nonfinancial information may also need to be disclosed in annual, periodic, or registration statements.[154] SEC regulatory guidance in Regulation S-K has been at the forefront of defining when a corporation must disclose certain nonfinancial information.[155] Only when nonfinancial information creates an event that will result in extensive costs for the company, like an oil spill, does the SEC require disclosure of nonfinancial information.[156] Although the SEC has the authority to mandate nonfinancial disclosures,[157] the SEC has yet to promulgate cybersecurity

---

[151] For example, a financial institution.

[152] For example, fraud or misconduct.

[153] *See* David Monsma & Timothy Olson, *Muddling Through Counterfactual Materiality and Divergent Disclosure: The Necessary Search for a Duty to Disclose Material Non-Financial Information*, 26 STAN. ENVTL. L.J. 137, 140–41 (2007).

[154] *See* Basic Inc. v. Levinson, 485 U.S. 224, 238–40 (1988) (declining to find merger discussions material but noting that materiality is a fact specific inquiry); *see also* United States v. Matthews, 787 F.2d 38 (2d Cir. 1986) (holding failure of defendant to disclose uncharged criminal conduct associated with his role as counsel for the same corporation despite running for a seat on the company's board of directors was not material requiring disclosure as it was purely qualitative in nature); SEC Staff Accounting Bulletin No. 99, 64 Fed. Reg. 45150 (Aug. 12, 1999) (providing accounting guidance when examining materiality and indicating qualitative factors must be considered if they create quantitative misstatements); Alison B. Miller, *Navigating the Disclosure Dilemma: Corporate Illegality and the Federal Securities Laws*, 102 GEO. L.J. 1647, 1684 (2014); Richard C. Sauer, *The Erosion of the Materiality Standard in the Enforcement of the Federal Securities Laws*, 62 BUS. LAW. 317, 355 (2007) (recognizing the qualitative materiality is a nonstarter, but in effect many disclosure requirements take on a noneconomic slant).

[155] *See* Miller, *supra* note 154, at 1655. Several Items within Regulation S-K have been cited as a means of mandating the disclosure of nonfinancial information. *See* Amy Deen Westbrook, *The Inadequate Disclosure of Business Conducted in Countries Designated as State Sponsors of Terrorism*, 39 SEC. REG. L.J. 15, 18 (2011) (noting that although both Item 503 (Risk Factors) and Exchange Act Rules 12b-20 (Additional Information) and 10b-5 (Employment of Manipulative and Deceptive Practices) can provide a catchall for disclosures, unless Regulation S-K contains a specific disclosure requirement, it is nearly impossible to impose a disclosure obligation on whether a company does business in countries on the State Sponsors of Terrorism list under the SEC's "materiality" requirement). Companies have begun disclosing nonfinancial information related to social responsibility efforts on a voluntary basis. See Adrian King et al., *Currents of Change: The KPMG Survey of Corporate Responsibility Reporting* 2015, KPMG (Nov. 2015), http://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Documents/kpmg-survey-of-corporate-responsibility-reporting-2015-O-201511.pdf. Companies doing business in the European Union must disclose a variety of nonfinancial information regardless of its materiality. *See* Council Directive 2014/95, 2014 O.J. (L 330) 1 (EU); *see also Sustainable Stock Exchanges 2014 Report on Progress*, SUSTAINABLE STOCK EXCHANGES INITIATIVE at 27 (2014), http://www.sseinitiative.org/wp-content/uploads/2012/03/SSE-2014-ROP.pdf.

[156] *See* Monsma & Olson, *supra* note 153, at 145; *see also Basic Inc.*, 485 U.S. at 238–40.

[157] *See* 15 U.S.C. §§ 78l(b)(1), 77j(c) (2016) (stating the SEC may promulgate regulations concerning any information necessary in the public interest or for the protection of investors);

disclosure regulations.[158] Thus, the decision to report cybersecurity issues is entirely voluntary.[159]

It is unlikely that the use of ephemeral communication would be considered material. However, corporations must be aware of disclosure requirements that did not previously exist, particularly in the environmental and social impact areas.[160] Where the nonfinancial information affects a

---

see also Patricia Romano, *Sustainable Development: A Strategy that Reflects the Effects of Globalization on the International Power Structure*, 23 HOUS. J. INT'L L. 91, 109 (2000).

[158] *See* U.S. SEC. & EXCH. COMM'N, CF DISCLOSURE GUIDANCE: TOPIC NO. 2-CYBERSECURITY (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm. Legal scholars and the SEC agree that there are competing interests in ensuring investors have sufficient information to instruct their investments, and not providing potential hackers with information enabling them to conduct further breaches. *See* Loren F. Selznick & Carolyn LaMacchia, *Cybersecurity: Should the SEC Be Sticking Its Nose Under This Tent?*, 2016 U. ILL. J.L. TECH. & POL'Y, 35, 70 (2016) (citing Will Daugherty, *The Evolving Landscape of Cybersecurity Disclosures*, 23 SECUR. LIT. J. 6, 6 (2013)).

[159] *See* 15 U.S.C. § 78q (2016); OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS, SEC. & EXCH. COMM'N, OCIE CYBERSECURITY INITIATIVE, IV.2 NAT'L EXAMINATION PROGRAM RISK ALERT (Apr. 15, 2014), https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert—Appendix—-4.15.14.pdf. Nonetheless, SEC guidance has been ineffective in encouraging voluntary disclosures because many companies fear disclosure. *See* Jennifer Booton, *Three Reasons Why Cyberattacks Don't Hurt Stock Prices*, MARKETWATCH (Apr. 3, 2015), http://www.marketwatch.com/story/3-reasons-why-cyberattacks-dont-hurt-stock-prices-2015-04-03; Danielle Gilmore & David Armillei, *The Future Is Now: The First Wave of Cyber Insurance Litigation Commences, and the Groundwork Is Laid for the Coming Storm*, ASPATORE, 2016 WL 1089828, at *6 (Feb. 2016) (discussing insurance litigation and coverage); *see also* Selznick & LaMacchia, *supra* note 158, at 53; *cf.* Steven L. Caponi, *Cybersecurity and the Board of Directors: Avoiding Personal Liability — Part II of III,* THOMSON REUTERS (Aug. 6, 2013), http://blog.thomsonreuters.com/index.php/cybersecurity-and-the-board-of-directors-avoiding-personal-liability-part-ii-of-iii/ (finding companies lose 5% in their share prices after disclosure of a breach). One area that could address the mandating of certain cybersecurity disclosures is through the SEC's April 2016 Concept Release, seeking input related to both financial and nonfinancial disclosures in Regulation S-K. *See* Sec. & Exch. Comm'n, SEC Solicits Public Comment on Business and Financial Disclosure Requirements in Regulation S-K, Press Release 2016-70 (Apr. 15, 2016), https://www.sec.gov/news/press-release/2016-70.html; *see also* The Cybersecurity Information Sharing Act of 2015, Pub. L. 114-113, 129 Stat. 2936, 6 U.S.C. § 1501–10 (2016) (permitting companies to monitor and implement defensive measures on their own systems and share information about indicators and defensive measures with others). But see concerns submitted by KPMG to the cybersecurity disclosure proposals at Sec. & Exch. Comm'n, Comments on Proposed Rule: Disclosure Update and Simplification, Exchange Act Release No. 33-10110, 2016 WL 6649529 (Oct. 9, 2016).

[160] *See* Ruth Jebe, *Sustainability Reporting and New Governance: South Africa Marks the Path to Improved Corporate Disclosure*, 23 CARDOZO J. INT'L & COMP. L. 233, 249, 251 nn.103–04, 115 (2015); *see also* National Ass'n of Manufacturers v. SEC, 800 F.3d 518 (D.C. Cir. 2015) (remanding case to district court to address First Amendment issues related to the SEC's disclosure requirements regarding whether a product was "conflict mineral"); Note, *Should the SEC Expand Nonfinancial Disclosure Requirements?*, 115 HARV. L. REV. 1433, 1437 (2002) (discussing the types of information shareholders wish to know); U.S. Sec. & Exch. Comm'n, Commission Guidance Regarding Disclosure Related to Climate Change (Feb. 2, 2010), http://sec.gov/rules/interp/2010/33-9106.pdf; Dynda A. Thomas, *SEC Conflict Minerals Rule Legal Challenge is Over – But Not For Good*, CONFLICT MINERALS LAW (Apr. 12, 2016), http://www.conflictmineralslaw.com/2016/04/12/sec-conflict-minerals-rule-legal-challenge-is-over-but-not-for-good/. Proper corporate procedures for the periodic disclosure of items entail "a system of internal accounting controls sufficient to provide reasonable assurances that—(i) transactions are executed in accordance with management's general or specific

company's financials, the SEC may pursue administrative enforcement actions.[161] Plaintiffs also may bring SEC fraud cases for failure to disclose, but their success may be limited.[162] To combat the corporate aversion of disclosure and to ensure shareholder protection, the SEC should mandate disclosure of whether companies permit the use of ephemeral media for corporate communications and whether companies have appropriate use and cybersecurity risk assessments in place. For companies whose policies fall short of nationally accepted best practices or who fail to report the use of the ephemeral media in daily business, shareholders should have private rights of actions against the board where the use leads to corporate liability, exposure, loss, or fraud.

IV. Transitory Communications Jeopardize Corporate Recordkeeping and Disclosure Liability

The use of ephemeral communications to conduct business negotiations or transactions could violate state and federal records retention and inspection regulations.[163] Private shareholder-plaintiff actions against companies are generally limited to securities fraud claims, discussed above, shareholder inspection rights enforcement, spoliation claims for lost evidence, and unfair practices for cybersecurity breaches affecting third parties.

A. Shareholder Inspection Rights

Documentary evidence is paramount for a variety of corporate and fiduciary obligations and must not be overlooked in the context of proper corporate management.[164] Shareholders have a right to inspect and review

---

authorization; (ii) transactions are recorded as necessary (I) to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements, and (II) to maintain accountability for assets." 15 U.S.C. § 78m(b)(2)(B) (2016).

[161] *See* Panjwani v. MobileIron, Inc., No. 3:15-cv-01984-VC (N.D. Cal. Oct. 5, 2015) (finding that although MobileIron failed to disclose in its registration statement that the devices of one of its customers were hacked despite using MobileIron's security application, the offending statements were merely forward-looking with protected cautionary language and no liability).

[162] *See* Doug Green, *Cybersecurity Securities Class Actions: A Wave or Trickle*, D & O Discourse (Mar. 17, 2015), http://www.dandodiscourse.com/2015/03/17/cybersecurity-securities-class-actions-a-wave-or-trickle/; *see also* Norah C. Avellan, *The Securities and Exchange Commission and the Growing Need for Cybersecurity in Modern Corporate America*, 54 Washburn L. J. 193 (2014).

[163] *See* Peter Sloan, *The Compliance Case for Information Governance*, 20 Rich. J.L. & Tech. 4, 5–6 (2014) (detailing the myriad of state and federal record retention obligations); News Release, Fin. Indus. Regulatory Auth. (FINRA), FINRA Fines Scottrade $2.6 Million for Significant Failures in Required Electronic Records and Email Retention (Nov. 16, 2015), http://www.finra.org/newsroom/2015/finra-fines-scottrade-26-million-significant-failures-required-electronic-records-and.

[164] *See* Browning Jeffries, *Shareholder Access to Corporate Books and Records: The Abrogation Debate*, 59 Drake L. Rev. 1087, 1104 (2011); *see also* Amalgamated Bank v. Ya-

corporate books and records if they can show they have a proper purpose for the request and the records are essential to their purpose.[165] "[A] stockholder's desire to investigate wrongdoing or mismanagement is a 'proper purpose.'"[166] Thus, a stockholder who can demonstrate "a credible basis from which [a] court can infer that [wrongdoing] or mismanagement may have occurred" has a right to inspect a corporation's books and records.[167]

Ephemeral communication hinders the number of available books and records for shareholder inspection. Depending on how corporate employees communicate, destroyed data may be the very data needed to detect wrongdoing. Thus, a shareholder should argue the investigation into the very use of ephemeral media as a common form of corporate communication is a proper purpose. If the company is unable to provide relevant data surrounding the rationale behind many of its significant corporate decisions, the use of the ephemeral media should form the basis of a breach of fiduciary duty claim, entitling shareholders to a derivative claim on behalf of the company for the improper use of transitory media.

B. Duty to Preserve

In addition to the right to inspect company records which necessarily implicates a system designed to retain documents related to the company's mission, there are additional retention and preservation issues surrounding ephemeral media. Ephemeral communications could contain information required to be preserved for potential litigation purposes. Substantial amend-

---

hoo! Inc., 132 A.3d 752, 786 (Del. Ch. 2016) (holding despite an exculpation provision, shareholders' demand for inspection should be upheld if shareholders can articulate proper purposes besides litigation, such as discussions for reform). Significantly, Delaware courts recognize that digital information is included in the right to inspect books and records. *See Amalgamated Bank*, 132 A.3d at 793.

[165] *See* Sabrina M. Hendershot, *Boards Beware: Delaware "Garners" Support for Fiduciary Exception to Attorney-Client Privilege in Section 220 Suits*, 40 DEL. J. CORP. L. 677, 687 (2016) (detailing a shareholder's rights under Delaware law to inspect a company's books and records).

[166] Seinfeld v. Verizon Communication, Inc., 909 A.2d 117, 121 (Del. 2006); *see also* Gabrielle Palmer, *Stockholder Inspection Rights and an "Incredible" Basis: Seeking Disclosure Related to Corporate Social Responsibility*, 92 DENV. L. REV. ONLINE 125, 127–28 (2015), http://www.denverlawreview.org/dlr-onlinearticle/2015/4/29/stockholder-inspection-rights-and-an-incredible-basis-seekin.html (noting examples of a proper purpose include claims that the controlling shareholder's assets were commingled with (1) the corporation, (2) the officers, and directors violated fiduciary duties, or (3) the board-approved excessive compensation).

[167] *Seinfeld*, 909 A.2d at 122–23. There are general limitations where inspection would reveal trade secrets or other confidential information. Corporate bylaws frequently limit a shareholder's right to inspect and may require confidentiality agreements. *See* Jeffries, *supra* note 164, at 1104; *see also Amalgamated Bank*, 132 A.3d at 786 (holding that despite an exculpation provision, shareholders can demand inspection if shareholders can articulate proper purposes besides litigation, such as discussions for reform); Ruari James O'Sullivan, *Skimming from the 2%: The Status of Georgia's Restrictions on Shareholder Access to Corporate Information*, 46 GA. L. REV. 835, 844 (2012) (stating that many states have similar inspection statutes to Delaware).

ments to the rules governing the preservation and disclosure of electronically discovered information (ESI) make clear that for Federal Rules of Civil Procedure Rule 37(e) to apply, there must first be a duty to preserve the ESI; the party must have failed to take reasonable steps to preserve the ESI; the ESI must be lost as a result of the failure; and the ESI cannot otherwise be obtained through alternate discovery.[168] If Rule 37(e) is implicated, then the court engages in a sanctioning analysis to determine "measures no greater than necessary to cure the prejudice."[169] The court is constrained in its sanctioning discretion in two ways. First, the complaining party must be prejudiced; and, second, the court's sanction can be no greater than necessary to cure the prejudice.[170] When a court determines the loss of ESI was intentional, it may impose more severe penalties.[171]

Under Federal Rules of Civil Procedure Rule 26(b)(1), "[p]arties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense—including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter."[172] Moreover, Rule 34(a) permits discovery of documents or electronically stored information if it is in the "responding party's possession, custody or control."[173] Information relevant to an ongoing lawsuit discussed through ephemeral media, which by its very nature is immediately deleted, places a company in a disadvantageous litigation posture because the officers and employees knew this form of communication would result in the immediate loss of relevant information, and yet, continued its use.

Rule 37's revisions help provide consistency among the varying court sanctions for the loss of discoverable information, particularly where courts give adverse inference instructions for the negligent or grossly negligent loss of information instead of only those cases where the responding party intentionally destroyed the information.[174] Thus, a party's bad faith and motive

---

[168] Federal Rules of Civil Procedure Rule 37(e) was amended effective December 1, 2015. The amendment eliminated the reference to safe harbors with respect to the loss of ESI resulting from "good faith" loss associated with routine record retention policies. Further, with respect to ESI, Rule 37 now supersedes state law spoliation standards. *See* FED. R. CIV. P. 37(e), Committee Notes on Rules—2015 Amendment advisory committee's note to 2015 Amendment.

[169] Sanctions might include: (1) precluding the destroying party from introducing evidence about the data, (2) allowing the prejudiced party to introduce evidence or argument about the prejudice; (3) instructing the jury how to evaluate the evidence relating to the ESI. *See* FED. R. CIV. P. 37(e)(1), 37(e) advisory committee's note to 2015 amendment.

[170] *Id.*

[171] A court may (1) presume the ESI was unfavorable to the destroying party when ruling on motion or bench trial; (2) instruct the jury the ESI can be presumed to have been unfavorable to the destroying party; or (3) dismiss the action or enter default judgment in favor of prejudiced party. *See* FED. R. CIV. P. 37(e)(2).

[172] FED. R. CIV. P. 26(b)(1).

[173] FED. R. CIV. P. 34(a).

[174] *See* Nuvasive, Inc. v. Madsen Medical, Inc., Civ. No. 13-2077, 2016 WL 305096, at *2 (S.D. Cal. Jan. 26, 2016) (finding that because the court did not find intentional failure to

continue to be relevant in assessing the type of sanction that may be appropriate.[175] Arguably, the mere use of ephemeral media could satisfy a bad faith motive. Corporate officers and directors who use applications like Cyber Dust risk that the information discussed need not be preserved. Without an appropriate risk assessment of the use of ephemeral media and an appropriate use policy for these communications, officers and directors are severely jeopardizing the company's future defense, and shareholder-plaintiffs should be able to hold them accountable for this mismanagement.[176]

The fact that conversations are maintained on social media or other digital devices does not eliminate the need to preserve the information where a "duty to preserve" exists.[177] This is true even if the person does not own or control the evidence.[178] Rather, the obligation is to notify the party who has custody of the evidence not to destroy it.[179] For ephemeral communications, and data in the cloud, the quandary is whether the corporation has "possession, custody or control" or the "legal right to obtain the documents on demand" sufficient to trigger its Rule 34 obligations.[180] Complications with access to third party information, like that stored in the cloud, might embolden a company to argue it is unable to preserve any of its information.

---

preserve text messages, an adverse inference instruction would be inappropriate under the new rules); *see also* Stinson v. City of New York, Civ. No., 10-4228, 2016 WL 54684, at *6–8 (S.D.N.Y. Jan. 5, 2016) (declining to impose an adverse inference instruction as there was no bad faith and the lost information was irrelevant, and declining to analyze the issues related to the Advisory Committee's discussion that negligence and gross negligence can never suffice to warrant such an instruction); *cf.* CAT3, LLC v. Black Lineage, Inc., 164 F. Supp. 3d 488, 488–89 (S.D.N.Y. 2016) (finding a court's inherent authority to craft sanctions is limited by the amendments to the Federal Rules of Civil Procedure particularly where spoliation is proven through clear and convincing evidence).

[175] *Nuvasive*, 2016 WL 305096, at *3 (citing Apple Inc. v. Samsung Elec. Co., Ltd., 888 F. Supp. 2d 976, 992 (N.D. Cal. 2012)) (stating that the degree of fault of the party destroying the evidence is relevant in determining sanctions); Roberson v. USAA Cas. Inc. Co., 2016 WL 5864431, at *5 (M.D. Fla. Sept. 22, 2016) (a finding of spoliation is warranted only if there is evidence of bad faith); *see also* Living Color Enter., Inc. v. New Era Aquaculture, Ltd., No. 14-cv-62216, 2016 WL 1105297 (S.D. Fla. Mar. 22, 2016) (holding that text messages constitute electronically stored information and are therefore governed by Federal Rule of Civil Procedure Rule 37(e)).

[176] *See In re* Krause, 367 B.R. 740, 767 (Bankr. D. Kan. 2007) (rejecting the routine deletion defense pre-Rule 37(e) revisions because the software itself, GhostSurf, was designed to clean the computers of all information from the start).

[177] Arnold, *supra* note 2; *see also* Sara Anne Hook & Cori Faklaris, *Oh, Snap!*, 63 FED. LAW 64 (May 2016); Clare Kealey, *Discovering Flaws: An Analysis of the Amended Federal Rule of Civil Procedure 37(E) and Its Impact on the Spoliation of Electronically Stored Evidence*, 14 RUTGERS J. L. & PUB. POL'Y 140, 174–75 (2016) (noting the complexity of corporate use of ephemeral media, like Vaporstream in the context of e-discovery).

[178] Hook & Faklaris, *supra* note 177.

[179] *Id.*

[180] Cindy Pham, *E-Discovery in the Cloud Era: What's A Litigant to Do?*, 5 HASTINGS SCI. & TECH. L.J. 139, 189 (2013) (discussing the difficulties in obtaining ESI from jurisdictions outside of the United States, such as the European Union).

However, it is clear that even metadata (data about data)[181] is required to be preserved.[182]

As noted above, the failure to preserve evidence implicates the federal rules, and the common law duty to preserve. In the Tenth Circuit, a plaintiff proves a common law spoliation (failure to preserve relevant evidence), where "'(1) a party has a duty to preserve evidence because it knew, or should have known, that litigation was imminent; and (2) the adverse party was prejudiced by the destruction of the evidence'" combined with a requisite state of mind.[183] Whether litigation is considered "imminent" is often a source of debate but includes times where a person has notice or should have known that evidence "may be relevant to future litigation."[184] To warrant the most severe sanctions of dismissal or an adverse inference instruction, something more than gross negligence is necessary.[185] This threshold would not be met simply through the use of ephemeral media without a prior duty to preserve. Without an affirmative obligation to disclose its use, the use of ephemeral media in daily communications in and of itself is not gross negligence.

Numerous potentially relevant pieces of information—including metadata—can be gathered from electronic media despite the communication's deletion.[186] Arguably, if a duty to preserve exists, the intentional use of ephemeral media in the normal course of business could satisfy the element of bad faith.[187] Accordingly, individuals should be aware that messages sent

---

[181] Metadata is not the substantive content of the information, but rather is the embedded information about, *inter alia*, who created the item, when it was created, where it was created, and any edits to the item. Generally, this information is automatically stored by the system in which it was created, but it can be deleted or overwritten in time either automatically by the system, or manually. *See The (2004) Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 5 SEDONA CONF. J. 151, 203 (2004).

[182] FED. R. CIV. P. 26 advisory committee's note to 2006 amendment, 34(a)(1)(A), 37(f) advisory committee's note to 2006 amendment; *see also* STEVEN S. GENSLER, 1 FEDERAL RULES OF CIVIL PROCEDURE, RULES AND COMMENTARY RULE 34 (2012) ("It seems clear that metadata falls within the scope of Rule 34 in that it constitutes electronically stored information.").

[183] Jones v. Norton, 809 F.3d 564, 580–81 (10th Cir. 2015) (citing Turner v. Pub. Serv. Co. of Colorado, 563 F.3d 1136, 1149 (10th Cir. 2009)). Rule 37 does not provide the standard for when preservation duties attach, and thus, is not applicable when evidence is lost prior to a duty to preserve for spoliation claims. However, to the extent state law spoliation standards conflict with Rule 37, the federal rules govern. *See* Living Color Enter., Inc. v. New Era Aquaculture, Ltd., No. 14-cv-62216, 2016 WL 1105297, at *4 (S.D. Fla. Mar. 22, 2016).

[184] Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc., 244 F.R.D. 614, 620 (D. Colo. 2007). Evidence warranting a duty to preserve includes filing of a lawsuit and may be triggered sooner if related to an incident that will likely result in litigation such as internal investigations, or where an adversary notifies party of potential litigation. See Zbylski v. Douglas Cty. Schl. Dist., 154 F. Supp. 3d 1146, 1163 (D. Colo. 2015).

[185] *See* Matthew Enter., Inc. v. Chrysler Grp. LLC, No. 13-cv-04236-BLF, 2016 WL 2957133 (N.D. Cal. May 23, 2016).

[186] *See The (2004) Sedona Principles*, *supra* note 181, at 201.

[187] The parties would have to anticipate that litigation was substantially likely based on their communications. *See Living Color Enter. Inc.*, 2016 WL 1105297, at *6 (noting that if

via ephemeral media never truly disappear. Metadata about when and to whom a particular message was sent, among other items, may be forensically obtained and provide fodder for a spoliation claim.

C. SEC Records and Disclosure Obligations

How does the duty to preserve correlate with an officer's or director's corporate oversight duty discussed earlier in this Article? One area where a lack of proper procedures, records, and oversight can cause individual, as well as corporate, liability is under the United States Foreign Corrupt Practices Act (FCPA), which contains accounting and anti-bribery provisions.[188] Significantly, federal law prohibits the destruction of evidence.[189] Such prohibition clearly applies to the use of ephemeral communication where the document's deletion impedes, obstructs, or influences an investigation.[190] The FCPA's auditing and accounting provisions contain a "books and records" provision and an "internal controls" provision.[191] The SEC and the Department of Justice (DOJ) enforce the FCPA.[192] As noted in the discussion of section 13b above, there is no scienter requirement for the recordkeeping violations prosecuted under the FCPA.[193]

The FCPA requires that a company's books and records fairly reflect in reasonable detail the corporate transactions; in order to ensure that internal controls provide "reasonable assurances," the transactions meet general or specific authorization and are recorded sufficiently to prepare financial state-

---

the deleted text messages occurred prior to a duty to preserve, Rule 37 liability does not attach).

[188] Foreign Corrupt Practices Act of 1977, 15 U.S.C. § 78dd-1 (2006). Both civil and criminal penalties are possible. 15 U.S.C. § 78dd-1 (2016) (prohibiting a United States individual or entity from bribing a foreign official); 15 U.S.C. § 78m(b)(2) (2012) (establishing recordkeeping and internal accounting controls to ensure compliance).

[189] 18 U.S.C. § 1519 (2016) ("Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.").

[190] *See id.*; *see also* 18 U.S.C. § 1512(c)(1) & (2) (2016); United States v. Jahedi, 681 F. Supp. 2d 430, 437 (S.D.N.Y. 2009) (noting Section 1512(c)(1) was enacted specifically for application in SOX related violations, but that its provision is not the only provision under which obstruction charges can be levied, noting 18 U.S.C. § 1503 likewise imposes liability).

[191] *See* 15 U.S.C. § 78m(b) (2016).

[192] *See In re* Key Energy Services, Inc. Sec. Litig., 166 F. Supp. 3d 822, 2016 WL 1305922, at *14 (S.D. Texas 2016) (dismissing shareholder class action for Rule 10b-5 and disclosure violations because of a failure to demonstrate the defendants knew of FCPA violations or participated in the violations; investigations alone are insufficient to establish the necessary scienter for liability); Susan Lorde Martin, *Compliance Officers: More Jobs, More Responsibility, More Liability*, 29 Notre Dame J.L. Ethics & Pub. Pol'y 169, 198 (2015) (noting the most common enforcement claims for improper corporate disclosures is under the FCPA).

[193] *In re* Key Energy Services, Inc. Sec. Litig., 2016 WL 1305922, at *15 (citing 15 U.S.C. § 78m(b)(2)(A)–(B) (2016)) (stating that there is no private right of action under the FCPA).

ments in accordance with generally accepted accounting principles (GAAP).[194] To determine whether a corporation's internal systems are adequate under the FCPA, the SEC evaluates (1) the board of directors' role, (2) whether the systems are properly communicated to the necessary parties, (3) who has responsibility to ensure the systems are working, (4) whether corporate personnel are competent, (5) the level of accountability for errors, and (6) the objectivity and effectiveness of the internal audit function.[195] Records are defined as "transcribed information of any type."[196] This definition necessarily includes ephemeral media. The use of ephemeral communications jeopardizes a company's internal control procedures by eliminating the ability to detect red flags, and subjecting the company to FCPA liability.[197]

There is no private right of action under the FCPA, only administrative and criminal enforcement. However, shareholder-plaintiffs should argue that FCPA failures establish a Rule 10b-5 securities fraud claim because the officers knew or should have known that the use of ephemeral media would interfere with the company's FCPA books and records obligations.[198] Shareholder-plaintiffs will struggle with private actions because even where companies fail to have adequate FCPA internal controls, courts have held their officers' SOX certifications were not false or misleading, eliminating any basis for liability.[199] Clearly, in light of judicial hesitancy to hold corporate officers and directors liable for failing to meet their corporate governance obligations, federal regulatory intervention is necessary.

V. Administrative Oversight Does Not Adequately Address Private Liability Exposure

Compliance with the myriad of regulations commences with the mindset of corporate leadership.[200] Effective compliance programs limit a com-

---

[194] *Id.* at *16.

[195] Amy Deen Westbrook, *Enthusiastic Enforcement, Informal Legislation: The Unruly Expansion of the Foreign Corrupt Practices Act*, 45 Ga. L. Rev. 489, 508–09 (2011).

[196] *In re* Key Energy Services, Inc. Sec. Litig., 2016 WL 1305922, at *15.

[197] *See, e.g.*, Stephenson v. Citco Group Ltd., 700 F. Supp. 2d 599, 622 (S.D.N.Y. 2010) (indicating allegations of an auditor's failure to follow GAAP procedures and ignoring red flags concerning a company's internal controls could lead to an inference of recklessness sufficient to establish an auditor's liability, but were insufficient in this case).

[198] *See In re* Key Energy Services, Inc. Sec. Litig., 2016 WL 1305922, at *14.

[199] *Id.* at *33.

[200] *See* Susan Lorde Martin, *Compliance Officers: More Jobs, More Responsibility, More Liability*, 29 Notre Dame J.L. Ethics & Pub. Pol'y 169, 186 (2015) (noting research shows a value-based approach to compliance rather than a compliance based approach is more effective in governing appropriate corporate behaviors modeled by upper management). The Sentencing Reform Act of 1984 created the United States Sentencing Commission, issuing federal guidelines for criminal penalties to incentivize the corporation to have "an effective compliance and ethics program." The Sentencing Reform Act of 1984, 28 U.S.C. §§ 991–98; 18 U.S.C. §§ 3551–3673 (1988); Patti B. Saris, *Remarks at the 12th Annual Compliance & Ethics Institute* 4 (Oct. 7, 2013), http:// www.ussc.gov/Guidelines/Organizational_Guidelines/Special_Reports/saris-remarks-annual-compliance-and-ethics-institute.pdf; *see also* Maurice E. Stucke, *In Search of Effective Ethics & Compliance Programs*, 39 J. Corp. L. 769, 787–89 (2014) (not-

pany's and its officers' and directors' liability.[201] Many companies have compliance officers who report directly to the board of directors to ensure effective compliance programs.[202] Where the company has systems in place that should "reasonably be expected to prevent and detect" violations, compliance officers are generally free from liability.[203] Arguably, the corporate use of ephemeral media severely restricts the company's ability to monitor their compliance programs and detect wrongdoing. In this regard, the administrative enforcement agencies should take the use of ephemeral media into consideration when assessing a company's compliance program. The existence of such corporate use should play a factor in negating a finding the system will "prevent and detect" violations.

In addition to the SEC's existing standards and state fiduciary requirements, other agencies seek to address cybersecurity issues in the corporate arena, yet provide minimal relief for private shareholder plaintiffs.[204] The most active of the federal agencies—besides the SEC and DOJ—regarding cybersecurity issues is the Federal Trade Commission (FTC) which investigates corporations that have failed to secure consumer's personal information, misused consumer's information, or violated children's privacy.[205] Section 5 of the Federal Trade Commission Act prohibits "unfair or deceptive practices in or affecting commerce."[206] To further its enforcement authority, the FTC institutes administrative enforcement actions that require "comprehensive privacy and security programs, biennial assessments by independent experts, monetary redress to consumers, disgorgement of ill-got-

ing very few firms have all of the requirements for an effective program and only the Department of Justice knows whether the advent of the programs have had a mitigating effect).

[201] U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(a)(2) (U.S. SENTENCING COMM'N 2016); *see also* Stucke, *supra* note 200, at 832. Having an ethics program alone is insufficient. Rather, the company must ensure monitoring to detect criminal conduct. However, the "failure to prevent or detect the instant offense does not necessarily mean that the program is not generally effective in preventing and detecting criminal conduct." *See* Martin, *supra* note 200, at 172 (discussing the US Sentencing Guidelines and mitigation of liability).

[202] *See* Martin, *supra* note 200, at 197 (generally compliance programs that are designed to detect misconduct are sufficient to avoid liability. However, the SEC has pursued individual compliance officers for their failure to properly supervise subordinates who they know have committed violations and has indicated there is potential for supervisory liability under Section 15(b) of the 1934 Act).

[203] *See* Martin, *supra* note 200, at 173, 191–92.

[204] *See, e.g.*, the Federal Communications Commission regulates national communications systems and providers and bases its recommendations on the NIST Framework. *Cyber Security and Network Reliability*, FED. COMM. COMM'N, https://www.fcc.gov/general/cyber-security-and-network-reliability (last modified Oct. 8, 2015); The Department of Homeland Security coordinates with federal, state, local and business communities to address and strengthen cybersecurity needs. *Cybersecurity Overview*, HOMELAND SECURITY, https://www.dhs.gov/cybersecurity-overview (last updated Sept. 27, 2016).

[205] *See* Jessica Rich, *2015 Privacy and Data Security Update* (Jan. 28, 2016 2:54 PM), https://www.ftc.gov/news-events/blogs/business-blog/2016/01/2015-privacy-data-security-update; *see also* Justin (Gus) Hurwitz, *Data Security and the FTC's Uncommon Law*, 101 IOWA L. REV. 955, 965 (2016).

[206] 15 U.S.C. § 45(a)(1) (2016).

ten gains, deletion of illegally obtained consumer information, and provision of robust notice and choice mechanisms to consumers."[207]

Failure to comply with an FTC administrative order can lead to civil monetary penalties.[208] A relevant example was *In the Matter of Snapchat, Inc*., in which the FTC and Snapchat settled an enforcement action alleging that Snapchat's claims that its messages disappeared were false.[209] It was found that the messages could be remotely stored and retrieved using a common file search tool and could also be intercepted during transmission or saved by the recipient without the sender's knowledge.[210] The FTC determined that Snapchat engaged in unfair trade practices in its advertising of the extent to which data is actually deleted after being reviewed by the recipient.[211] It also determined that Snapchat overstated other products' capabilities to detect whether the recipient captured the information that was sent and the steps taken to protect unauthorized disclosure.[212] The consent decree required Snapchat to establish a comprehensive privacy program, including monitoring and reporting obligations for twenty years.[213]

More recently, the Third Circuit Court of Appeals upheld the FTC's authority to regulate in this area[214] and determined that a company acts un-

---

[207] Fed. Trade Comm'n, Privacy and Data Security Update: 2015 (Jan. 2016), https://www.ftc.gov/reports/privacy-data-security-update-2015; *see also* Rich, *supra* note 205, at 979–80 ((noting the FTC has enforcement authority over "unfairness" in trade practices, but courts dispute the FTC's attempt to create binding common law for data security practices). The FTC also provides practical guidance. *See* Fed. Trade Comm'n, Start with Security: A Guide for Businesses (June 2015) https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.; *cf*. Fed. Trade Comm'n, Big Data: A Tool for Inclusion or Exclusion? Understanding The Issues (Jan. 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf. The FTC's Bid Data Report has been described as "a concise but essential guide to corporate big data behaviors in the increasingly hawkish view of the FTC." Lisa Brownlee, *FTC Releases Its Bid Data Bible,* Forbes (Jan. 7, 2016, 7:11 AM), http://www.forbes.com/sites/lisabrownlee/2016/01/07/ftc-releases-its-big-data-bible/#4a2f374e4c69. As a result of these efforts, the FTC issued further guidance on October 25, 2016 to companies addressing the need to examine the entity's network, and to notify shareholders, consumers, and law enforcement when a breach occurs. *See* Fed. Trade. Comm'n, Data Breach Response: A Guide for Business (Sept. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf; *see also* Lisa Weintraub Schifferle, *Responding to a data breach?*, Fed. Trade Comm'n: Bureau of Consumer Prot. (Oct. 25, 2016 2:14 PM).

[208] *Id.*

[209] Decision and Order, *In re* Snapchat, Inc., No. C-4501, (Fed. Trade Comm'n, Dec. 23, 2014), https://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf.

[210] Complaint at ¶ 9–12, 14, 18–19, *In Re* Snapchat, Inc., No. C-4501 (Fed. Trade Comm'n, Dec. 23, 2014), https://www.ftc.gov/system/files/documents/cases/141231snapchat cmpt.pdf.

[211] *Id.* at ¶ 9–15, 16–17.

[212] *Id.* at ¶ 15, 19.

[213] Decision and Order at Part III, *In re* Snapchat, Inc., No. C-4501, (Fed. Trade Comm'n, Dec. 23, 2014).

[214] *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 247 (3d Cir. 2015) (upholding the FTC's authority regarding data security, but suggesting the necessary proof to establish unfair practices that "causes or is likely to cause substantial injury" is a high bar); *see also* Kacy Brake, *FTC and Wyndham Settle Data Security Allegations*, Alston and Bird Privacy

fairly when the practice will likely cause "substantial injury," is unavoidable by the consumers, and is not outweighed by countervailing benefits to consumers or competition.[215] The Third Circuit indicated that a "company does not act equitably when it . . . exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business."[216] Therefore, unfairness can exist even prior to an actual injury.[217]

Despite the FTC's success in its administrative actions, individual plaintiffs have not been as fortunate.[218] For example, a class action was dismissed in a Maryland federal district court despite the plaintiffs' allegations that CareFirst, Inc. failed to protect its customer's personal information and that failure resulted in a cyber attack.[219] The court reasoned that the plaintiffs failed to allege any actual injury despite the allegation that the company failed to encrypt personal information for over 1.1 million customers and

---

AND DATA SECURITY BLOG (Dec. 15, 2015), http://www.alstonprivacy.com/ftc-and-wyndham-settle-data-security-allegations/.

[215] *Wyndham*, 799 F.3d at 243–44.

[216] *Id.* at 246. Merely because the company's actions are not the nearest or "most proximate cause of an injury" does not eliminate the potential for corporate liability. The fact a company is likewise a victim of the breach is not an excuse.

[217] *See id.*; *see also In re* LabMD, Inc., No. 9357, 2016 WL 4128215, at *14–16 (F.T.C. July 28, 2016) (finding by the FTC Commission on appeal that LabMD had acted unfairly through its unreasonable cybersecurity practices despite the original administrative law judge's ruling that the practice injured or was likely to cause substantial consumer injury because a large number of consumers' sensitive information included social security numbers, insurance policy numbers, and medical test results which can result in potential medical and identity theft as well as shame and embarrassment). However, the Eleventh Circuit Court of Appeals has stayed the FTC's enforcement action, noting the FTC's interpretation of what is likely to cause substantial consumer injury is potentially unreasonable in light of the lack of actual injury to consumers over the past two years. *See* LabMD, Inc. v. Fed. Trade Comm'n, No. 16-16270-D (11th Cir. Nov. 10, 2016), http://www.steptoe.com/assets/attachments/4934.pdf (order staying FTC enforcement action pending appeal). The Federal Communications Commission issued a Notice of Proposed Rule Making with Comment deadline of June 27, 2016 to ensure consumer privacy protections and data breach notification standards in *In re* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 2500, 2016 WL 1312850, at *9 (Apr. 1, 2016).

[218] *See generally In re* The Home Depot, Inc., 2015 WL 3814441 (N.D. Ga. May 27, 2015) (initial complaint that board of directors interfered with upgrading data security despite numerous and specific red flags. The parties later settled for a multi-million dollar settlement fund, additional security training, and practices and monitoring services, 2016 WL 1298002 (Mar. 7, 2016)); Palkon v. Holmes, No. 2:14-01234 (SRC), 2014 WL 5341880, at *1 (D.N.J. 2014) (dismissing at motion to dismiss stage because plaintiffs failed to allege sufficient facts to overcome the business judgment rule); Kulla v. Steinhafel, No. 14-cv-00203, 14-cv-00261, 14-cv-00266, 14-cv-00551, 2014 WL 2116594 (D. Minn. 2014) (derivative suit originally filed against directors for failure to act despite numerous data security risks at Target stores was ultimately dismissed on July 7, 2016 after a special litigation committee determined it was not in the best interest of Target to pursue these claims, which the shareholder-plaintiffs did not challenge); *Davis v. Steinhafel*, No. 14-cv-203 (PAM/JJK) (D. Minn. July 7, 2016), http://www.dandodiary.com/wp-content/uploads/sites/265/2016/07/Target-dismissal-order.pdf (granting motion to dismiss); Kevin LaCroix, *Target Corporation Cybersecurity-Related Derivative Litigation Dismissed*, THE D&O DIARY (July 9, 2016), http://www.dandodiary.com/2016/07/articles/cyber-liability/target-corporation-cybersecurity-related-derivative-litigation-dismissed/.

[219] Chambliss v. Carefirst Inc., No. 15-2288, 2016 WL 3055299, at *6 (D. Md. May 27, 2016).

was on prior notice for its security problems.[220] Regulatory intervention is needed in the cybersecurity arena to ensure that officers and directors are held accountable for their continuing failure to properly educate themselves about their companies' cybersecurity uses and risks. At a minimum, companies must be compelled to thoroughly assess the use of ephemeral media, the associated risks, relevant best practices, and cybersecurity protections. Courts, through private rights of action and administrative enforcement, must provide redress for the failure to meaningfully engage in these risk assessments. In a world of ever changing technology, courts should not be complicit in allowing officers and directors to satisfy their obligations through cursory discussions of technology and cybersecurity. Rather, consequential regulations and penalties are needed to incentivize proper corporate management.

VI. Accountability for the Use of Ephemeral Media in Our Scenario and Conclusion

Consider the ABC, Inc. scenario from the beginning of this Article in light of the jurisprudence examined. Arguably, ABC's officers breached several duties to the company: (1) there was no corporate BYOD policy in place, exposing the company to a cybersecurity attack; (2) there were no parameters regarding permissible corporate discussions on ephemeral media despite a pending sexual harassment claim; (3) the officers failed to fully inform the board and the auditor of the business and prevalent use of ephemeral media; and (4) the officers failed to timely advise the board of the data breach. The Board and auditor failed: (1) to fully assess the company's internal methods of communication and cybersecurity risks; (2) to implement and ensure compliance with acceptable use and BYOD policies; (3) to disclose the cybersecurity risks involved in their officers' preferred methods of communication to the trading public; and (4) to timely disclose the data breach, exposing social security numbers, which likely will result in lawsuits and federal investigations.

Despite all of these failures, a shareholder-plaintiff would struggle in suing the officers, directors or auditor under the business judgment rule and

---

[220] *Id*. (noting the information did not contain social security numbers or credit card information); *see also* Kevin LaCroix, *Dismissal Granted in Cyber Breach-Related Derivative Suit Filed Against Wyndham Officials*, The D&O Diary (Oct. 21, 2014), http://www.dandodiary.com/2014/10/articles/cyber-liability/dismissal-granted-in-cyber-breach-related-derivative-suit-filed-against-wyndham-officials/ (dismissing the case based on application of the business judgment rule because the board did discuss the breaches and security issues on at least sixteen occasions). Whether shareholder-plaintiffs have federal court standing depends on whether they suffered an "injury in fact" which the United States Supreme Court recently clarified can be based on the violation of one's "statutory rights" rather than the rights of other people. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016). Accordingly, to ensure standing, regulations and statutes should mandate disclosure of whether a corporation utilizes ephemeral media and when a data breach occurs based on the use of such media, shareholder-plaintiffs should have standing to sue.

Caremark oversight standards. There is no evidence of bad faith or red flags that are so obvious that the failure to correct them can be viewed as a conscious disregard of fiduciary duties. Moreover, neither state or federal books and records regulations nor the duty to preserve obligations are implicated as there is no evidence that pending litigation was discussed in the ephemeral media and no criminal wrongdoing exists. The Board took immediate remedial action once it learned of the breach. Arguably, the Board and the auditor were extremely negligent in not assessing their IT risks prior to the breach, specifically regarding the use of ephemeral communications. Further, the officers were negligent in not disclosing the data breach timely. Nonetheless, according to current jurisprudential thought, a shareholder-plaintiff has not suffered an articulable injury and no individual liability attaches. The most likely entities that could enforce any action against ABC and its officers, directors and the auditor would be the SEC under its books and records authority, and the FTC for unfair and deceptive trade practices.

Certainly, ephemeral media has its place in daily conversations and its use should not necessarily be prohibited in the corporate context. However, accountability for the lack of oversight and proper use of such media should exist. Ostensibly, corporate management satisfies their duties to shareholders and the trading public simply through a shallow discussion of cybersecurity issues. They do not, however, truly examining whether their internal systems comply with best practices or whether their IT systems and methods of communication expose the company to a variety of legal risks. Officers and directors must take affirmative steps to limit the methods of corporate communication and ensure employees have a full understanding of when and what types of communication is appropriate in the ephemeral media context. Without regulatory intervention, the ability to detect wrongdoing, preserve relevant evidence, and prevent cybersecurity risks is severely restricted and will not keep pace with changing technological advances. Although administrative enforcement provides some measure of corporate accountability, it falls short. Shareholders should be entitled to avenues of available recourse if their officers and directors fail to properly manage and oversee their companies.

Accordingly, current proposed legislative amendments and existing SEC cybersecurity guidance should be modified to require companies to disclose whether they permit business discussions over ephemeral media. Companies should also be made to disclose whether and to what extent cybersecurity risks have been assessed with such use, whether acceptable use policies concerning such media have been implemented, and how the company is able to determine compliance with laws despite the use of such media. Further, auditing standards should be revised to specifically address whether a company utilizes ephemeral media and determine how random sampling could capture evidence of material weaknesses in the company's financial statements. The DOJ and SEC need to address whether this method of communication exposes a company to FCPA compliance and securities

fraud issues. And, finally, specific avenues of recourse need to be made available through state and federal legislation for shareholder-plaintiffs to hold companies liable when their board fails to properly oversee the use of ephemeral media in light of the above risks.