# THE IMPLICATIONS OF A JEOPARDY COMPUTER NAMED WATSON: BEATING CORPORATE BOARDS OF DIRECTORS AT FIDUCIARY DUTIES?

Roger M. Groves†

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.</td>
<td>INTRODUCTION</td>
<td>378</td>
</tr>
<tr>
<td>II.</td>
<td>ELECTRONICALLY STORED INFORMATION IN LITIGATION</td>
<td>379</td>
</tr>
<tr>
<td></td>
<td>A. The Scope of the E-Discovery Problem and Underpinnings for Forensic Analytics</td>
<td>380</td>
</tr>
<tr>
<td></td>
<td>B. Platforms</td>
<td>382</td>
</tr>
<tr>
<td></td>
<td>C. Enronic Embryonics of Forensic Analytics</td>
<td>383</td>
</tr>
<tr>
<td></td>
<td>D. State of the Science</td>
<td>385</td>
</tr>
<tr>
<td></td>
<td>E. Predictive Analytics</td>
<td>387</td>
</tr>
<tr>
<td></td>
<td>F. E-mail Analytics</td>
<td>391</td>
</tr>
<tr>
<td></td>
<td>G. Contextual Forensic Evidence in Litigation</td>
<td>392</td>
</tr>
<tr>
<td>III.</td>
<td>ISSUES OF PROCEDURE AND ADMISSIBILITY: LITIGATION HOLD AND SEARCH PROTOCOL</td>
<td>394</td>
</tr>
<tr>
<td>IV.</td>
<td>SUBSTANTIVE CLAIMS AGAINST DIRECTORS FOR BREACHES OF FIDUCIARY DUTIES</td>
<td>399</td>
</tr>
<tr>
<td></td>
<td>A. Plaintiffs' Quiver of Claims—A Wide Array of Theories and Causes of Action</td>
<td>399</td>
</tr>
<tr>
<td></td>
<td>B. The Defendants</td>
<td>403</td>
</tr>
<tr>
<td></td>
<td>C. Defining the “Duty” in the Digital World</td>
<td>404</td>
</tr>
<tr>
<td></td>
<td>D. Data Recovery and Analysis</td>
<td>405</td>
</tr>
<tr>
<td></td>
<td>E. The Preeminent Importance of Metadata and Unveiling Attempts to Destroy Evidence</td>
<td>407</td>
</tr>
<tr>
<td></td>
<td>F. Correlating Forensic Analytics with Fiduciary Duty Claims</td>
<td>410</td>
</tr>
<tr>
<td></td>
<td>G. Forensic Behavioral Analytics</td>
<td>413</td>
</tr>
<tr>
<td></td>
<td>H. Securities Claims</td>
<td>417</td>
</tr>
<tr>
<td></td>
<td>I. The Danger of Adverse Inferences</td>
<td>418</td>
</tr>
<tr>
<td></td>
<td>J. Maximum Director Protections</td>
<td>420</td>
</tr>
<tr>
<td></td>
<td>K. Financial Reporting Enhancements</td>
<td>422</td>
</tr>
<tr>
<td></td>
<td>L. The Impact of Social Media</td>
<td>423</td>
</tr>
<tr>
<td>V.</td>
<td>CONCLUSION</td>
<td>424</td>
</tr>
</tbody>
</table>

† Professor of Law, Florida Coastal School of Law, former tax judge and equity partner at Howard & Howard, Attorneys PC. Emphatic appreciation is extended to Nicole A. Groves and research assistant Tier Brown for their valuable contributions.
Computers are getting better at mimicking human reasoning—as viewers of ‘Jeopardy!’ found out when they saw Watson beat its human opponents . . . [This] software provides a way to better understand the internal workings of corporations he sues, particularly when the real decision makers may be hidden from view. Now artificial intelligence software has taken a seat at the negotiating table.¹

I. INTRODUCTION

Can my employer look at my e-mails, cell phone calls, instant messages, Facebook, and Twitter accounts over the past two years and know when I lied? Can they know when I edited documents uncharacteristically as part of a cover up? If I am on the board of directors of a corporation, can my e-mails reveal our decision-making anomalies? If so, how does that play out in litigation? Ask Enron executives. Welcome to the world of forensic evidence analytics.²

While the story of Enron has largely been written, the Enron litigation documents are unwitting sunken treasures that are still being explored. Millions of documents, including five million messages, termed electronically stored information (“ESI”), from the Enron litigation have provided an opportunity for software developers to commence a cottage industry.³ The industry is forensic examination of ESI to discover trends and make findings as to who did what in the company. The industry of forensic analytics found its oasis in those Enron documents, now known as the “Enron Corpus.” Pretrial discovery is now thrust onto a technological landscape the law is struggling to traverse. The struggle is due in large part to the volume of ESI and the value of cutting edge software that analyzes documents for behaviors of computer users in more provocative and innovative ways than previously encountered.

² See Press Release, Cataphora, Inc., Cataphora Reveals Latest Advanced Social Network Data Analysis Technologies (July 6, 2009), available at http://www.cataphora.com/releases/release/cataphora-reveals-latest-advanced-social-network-data-analysis-technologies/ (indicating how analytics references software products that construct elaborate models of organizational behavior making deviations from normal behavior easier to identify); see also NAT'L VISUALIZATION & ANALYTICS CTR., U.S. DEP'T OF HOMELAND SEC., ILLUMINATING THE PATH: THE RESEARCH AND DEVELOPMENT AGENDA FOR VISUAL ANALYTICS (James J. Thomas & Kristin A. Cook eds., 2005), available at http://nvac.pnl.gov/docs/RD_Agenda_VisualAnalytics.pdf (providing that visual analytics is another phrase to refer to a reasoning process created by software that maximizes a human’s ability to perceive, comprehend, and reason about complicated and dynamic situations and data). Synonymous terms to visual analytics are forensic analytics or social analytics.
³ Markoff, supra note 1.
The e-discovery ambiguities and uncertainties provide an opportunity for counsel to manipulate or take advantage of forensic investigations. This Article examines the potential exploitation of e-discovery forensic tools by a corporation’s shareholders who suspect their board members have breached their fiduciary duties. Accordingly, Part One highlights the background and evolution of e-discovery. Part Two presents a more detailed discussion of specific types of forensic evidence as applied to litigation, and potentially, fiduciary duty claims. Finally, Part Three applies the various forms of forensic analytics to shareholders’ breach of fiduciary duty claims.

II. ELECTRONICALLY STORED INFORMATION IN LITIGATION

The tremendous growth in the costs to produce volumes of electronically stored information (“ESI”) as part of pretrial discovery is well documented. The failure of business organizations to preserve ESI, the failure to develop new skills to preserve ESI, and counsel attempts to abuse the discovery process to prevent collection or create unreasonable demands for the information have all led to confusion and judicial sanctions. As stated by one group of experienced e-discovery litigators, “The resources of clients, counsel and courts are quickly overtaxed in this new era when counsel make unreasonable demands for information or fail to carefully think through the process of searching for and collecting ESI.”

In response to this techno-legal morass, the Federal Rules of Civil Procedure (“FRCP”) were amended to specifically guide attorneys concerning their duties in requesting and responding to discovery. Not

4. One commentator estimated the cost to search e-mails at two billion dollars based on a total universe of one billion e-mail records. See George L. Paul & Jason R. Baron, Information Inflation: Can the Legal System Adapt?, 13 Rich. J. L. & Tech. 10 (2007) (discussing the challenges of increased information on litigation); see also Robert C. Manlowe et al., Paradigm Shifts in e-Discovery Litigation: Cooperate or Continue to Pay Dearly, 78 Def. Couns. J. 170 (2011) (providing a discussion on the increased costs in pretrial discovery of ESI).

5. See Manlowe et al., supra note 4, at 170 (explaining how businesses, lawyers, and ESI have affected judicial proceedings).

6. See id.

7. The Scheduling Order section of the Federal Rules was amended to include provisions for the “discovery or disclosure of electronically stored information.” Fed. R. Civ. P. 16(b)(3)(B)(iii). Any agreements by the parties regarding an assertion of privilege or document protection post-disclosure are to be included in the scheduling order. Fed. R. Civ. P. 16(b)(3)(B)(iv). And more notably, federal courts must receive a report from the attorneys as part of their Rule 26(f) conference that includes those e-discovery items. See Fed. R. Civ. P. 26(f) (providing the rules regarding disclosure and discovery for federal civil procedure). Rule 26(f) specifically states that the conferences include “any issues relating to disclosure or discovery of electronically stored information.” Fed. R. Civ. P. 26(f)(3)(C).
surprisingly, the FRCP could not cure all the potential ambiguities and crafty tactics in litigation, so numerous federal court decisions attempt to clarify these e-discovery issues. Some cases provide sanctions for discovery improprieties, some do not, and others select or threaten an array of other remedies for e-discovery violations.

A. THE SCOPE OF THE E-DISCOVERY PROBLEM AND UNDERPINNINGS FOR FORENSIC ANALYTICS

The Advisory Committee ("Committee") tasked with amending the Federal Rules of Civil Procedure to address e-discovery issues identified four major reasons why amendments were necessary. All of those reasons provide background for why forensic analytics is relevant. These reasons link forensic evidence with the potential for increasing the risk of fiduciary liability for corporate board members.

The first reason for the e-discovery amendments is that the sheer volume of electronically stored information ("ESI") dwarfs any traditional concept of scope known in the primarily paper record era. According to the Committee's findings, "[N]inety-five percent of all information is now generated in digital form, [and] all document discovery is or will soon be e-discovery." A major corporation may easily have 10,000 tapes of information. Just one tape is the equivalent of a "200-mile high stack of paper".

The second impetus for e-discovery rules is the "dynamic nature" of ESI, since it continues to grow and evolve. Eerily similar to fictional horror films of man versus machines, computers automatically create and store information without human operator advice or knowl-

---


9. See Zubulake v. UBS Warburg LLC, 220 F.R.D. 212 (S.D.N.Y. 2003); see also Banc of Am. Sec., 685 F. Supp. 2d at 456. See generally Shira A. Scheindlin, E-Discovery: The Newly Amended Federal Rules of Civil Procedure, in MOORE'S FEDERAL PRACTICE: PROPOSED AMENDMENTS ON E-DISCOVERY 1 (2006). The Zubulake and Banc of Am. Sec. cases are prominent cases in e-discovery litigation that both addressed spoliation of electronic documents and various remedies related to such destruction, including potential sanctions or adverse inferences.

10. See Scheindlin, supra note 9, at 1, 2 (explaining that the Advisory Committee on Civil Rules is a Committee of the Judicial Conference of the United States, composed of two federal appellate judges, four federal district judges, a federal magistrate judge, a state court judge, a law professor, and five practicing attorneys). Judge Shira A. Scheindlin was a member of that Committee.

11. Scheindlin, supra note 9, at 2.


13. See id.

edge. Importantly, a corporate director from the typewriter era may not know that the modern computer has "metadata," which can identify information about the user well beyond the words typed into that computer. Metadata can identify the creator and when the information was last accessed and last edited.

Saliently for this paper, metadata also includes "clues to human behavior." As artfully stated by one author, "[Metadata is] . . . the electronic equivalent of DNA, ballistics and fingerprint evidence, with a comparable power to exonerate and incriminate. Metadata sheds light on the context, authenticity, reliability and dissemination of electronic evidence . . . ." The utility of this metadata, particularly its potential to "exonerate and incriminate," is brought to fruition through the forensic analytics discussed in this Article. The subject to be exonerated or incriminated can be a corporate director. Accordingly, metadata is a vital aspect of forensic analytics and will be discussed in greater detail below.

The third reason for e-discovery amendments is simply because unlike paper records, electronic records are practically impossible to delete. A corporate employee who hits the delete key only moves the data to a more remote location. Though more expensive or time consuming to obtain, the data is not only recoverable but also discoverable. A corporate officer or board member, therefore, may have deleted an item that nonetheless can be part of forensic analytics, the very process that may lead to incriminating inferences or conclusions regarding that person.

The fourth unique challenge brought by ESI is the added complexity required to process document retrieval, restoration, and translation. In an age of accelerated technological advances, it is entirely possible that ESI was initially stored in devices that are now obsolete or part of an inaccessible or poorly organized prior format. Translating information to current formats may be costly and time consuming. These retrieval burdens add to the burden of being a director

15. See id.
16. See id.
17. See id. at 2 n.4.
18. See id.
19. See id. at 3.
20. See id.
21. See Antioch Co. v. Scrapbook Borders, Inc., 210 F.R.D. 645, 652 (D. Minn. 2002); Scheindlin, supra note 9, at 3 (noting that recovering deleted information may come at significant expense and time).
22. Scheindlin, supra note 9, at 3.
23. See id.
24. See id.
defendant who is obligated to produce ESI from obsolete storage devices.

For defendant directors, the retrieval and translation problems may be compounded by the possibility of multiple plaintiffs. In this Article, shareholders are contemplated as plaintiffs, but a director’s fiduciary duties run to both the shareholders and the corporation. The corporation, therefore, could conceivably be another plaintiff along with the shareholders, both with separate counsel, teaming up with e-discovery requests. Perhaps more importantly, they could combine resources to retain high quality forensic experts to investigate and report evidence of a director’s misdeeds. An individual director could easily be overmatched in the arms race for forensic experts. The consequences of losing the forensic war can be grave.

The translation process necessarily involves changing old data into new formats. Forensic analytics is another form of translation from old to new. As will be discussed below, forensic analytics is not confined to the mere retrieval of “as is” electronic documents. Forensic experts can also generate additional findings from data—findings that may identify the computer user’s behavior patterns. Those patterns are therefore documentary sources for fiduciary duty liability not otherwise contemplated by corporate officers, employees, or directors.

B. Platforms

In addition to the above, unique challenges for electronically stored information (“ESI”), there is a challenge given the various forms or “platforms” within which ESI is stored. A stand-alone desktop computer connected to an office database is but one source of a user’s stored information. ESI may also be contained in “personal digital assistants (PDA’s), laptops, thumb drives, telephone calls placed through the [I]nternet (i.e. voice over internet protocol or VoIP) smart cards and mobile phones.” Forensic analytics can examine data from all those sources.

A corporate director subject to a plaintiff’s investigation will have his or her communications analyzed from an unprecedented array of

25. The Model Business Corporations Act (“MBCA”) provides various sections under which shareholders may bring suit against directors, including circumstances where a director is involved in a conflict of interest transaction. MODEL BUS. CORP. ACT § 8.63(a) (2005).

26. There may be an indemnification provision in the articles of incorporation that can shield directors from some forms of liability. As a contractual matter, the directors may find indemnification does not cover certain acts that could bring a breach of fiduciary claim, such as a director’s individual fraud, embezzlement, or other felony.

27. See SCHEINDLIN & CAPRA, supra note 12, at 40. iPods are a common example of personal digital devices that store retrievable data subject to potential discovery.
comprehensive sources. Directors with questionable activities may avoid excoriating communications on the laptop but still have damaging information revealed from an alternate source. Plaintiffs' forensic investigators and counsel have numerous opportunities for corroboration with the increased reliability of forensic findings.

C. ENRONIC EMBRYONICS OF FORENSIC ANALYTICS

Forensic analysis in litigation owes much of its development to the recent corporate scandals. In the fall of 2001, Kenneth Lay, the Chief Executive Officer ("CEO") of Enron Corporation, was warned of an "elaborate accounting hoax" that "disguised fraud on a magnificent scale." Enron publicly disclosed a record nosedive in profits for the fourth quarter of that year, but executives nonetheless distributed more than $100 million in bonuses to themselves. A host of criminal prosecutions followed against Kenneth Lay, former President and CEO Jeff Skilling, and Chief Accounting Officer Richard Causey. Prior to, during, and after those criminal prosecutions, personal liability for breaches of fiduciary duties was looming over the Enron executives.

In light of impending liability, some corporations have a paper-shredding party in anticipation or conjunction with their pity party. This was not completely so at Enron. As described by one technology observer, "[A]s the . . . corporation came to a disintegrating halt, one road kill left behind was to become a significant gift to the science of artificial intelligence." It just so happened that the Federal Energy Regulatory Commission ("FERC") was one of the many federal agencies that investigated Enron. Through its investigation, the FERC discovered a large amount of company e-mails that became part of the public record. An enterprising researcher bought a copy of the database for $10,000 to use in his research in machine learning and natural language processing. That database has become known as the Enron Corpus.

The researcher made the Enron Corpus available to others, including Carnegie Mellon University. Carnegie used the database to explore how humans, as opposed to machines, decide to organize data.

29. See id. (tracking the trials of the 46 defendants and respective verdicts and guilty pleas with respect to suits against Enron executives).
31. Id. at 67.
32. See id. (providing the name of the researcher as Mr. Andrew McCallum at the University of Massachusetts).
33. See id. (describing the Corpus that includes 619,446 messages from 159 different users).
and classify messages. This was accomplished in large part by analyzing user threads and folders. Other researchers used the Enron Corpus to develop the "Enronic E-mail Visualization and Clustering Tool" designed to create "graph-based visualizations of social networks within Enron, based on e-mail interactions between users." Another group of researchers used the Enron Corpus to test "Link Discovery" techniques, which were used to "ferret out fraud and terrorist activities" based on the electronically stored information ("ESI") of the company.

Corporate directors are charged with statutory oversight functions in the many states that follow the Model Business Corporation Act. The board of directors, therefore, is necessarily in communication with committees, auditors, accountants, in-house counsel, and other key personnel. The failure to provide adequate oversight of those entities may give rise to a breach of fiduciary duties claim. The visualization of social networks that forensic experts developed from the Enron Corpus appear easily translatable into an analysis of business networks between directors and the personnel over which they must maintain oversight functions. Similarly, "Link Discovery" tools designed to connect atypical communication patterns could be configured to identify corporate director fraud, which is a factual basis for fiduciary duty breaches.

These Enron Corpus-tested methodologies were just the beginning. As more dramatically stated, the testing of the Enron Corpus data "has become an unending academic autopsy courtesy of one of the most spectacular corporate deaths in modern times."

34. See id.
35. See id.
36. See id. (stating that the University of California at Berkeley conducted research).
37. See id. (stating that the University of Southern California conducted research).
38. See Robert W. Hamilton et al., Cases and Materials on Corporations Including Partnerships and Limited Liability Companies 653 (11th ed. 2010) (providing that the scope of fiduciary duties is governed primarily by state law). The MBCA includes a provision that directors have a duty of due diligence, that is to become "informed in connection with their decision-making function," and a duty of reasonable oversight. Model Bus. Corp. Act § 8.30(b) (2005).
39. Shareholders can file an action to remove a director "engaged in fraudulent conduct with respect to the corporation or its shareholders." Model Bus. Corp. Act § 8.09(a) (emphasis added). Fraud is inconsistent with a director's obligation to act in good faith and within the best interests of the corporation. Model Bus. Corp. Act § 8.30(a).
40. Castelluccio, supra note 30, at 68.
D. **State of the Science**

Forensic evidence based on artificial intelligence and related software programs is irrelevant in fiduciary duty litigation unless there is a real threat and opportunity that an expert witness’s theory, testimony, and documentary evidence will be accepted. Accordingly, the Federal Rules of Evidence should be examined to ascertain whether there is a recognized scientific foundation for these theories, testimony, and documents.

A threshold question is what is the scientific foundation for the forensic evidence and how did it evolve specifically in the litigation context beyond Enronic research? In what has been termed “a different kind of business intelligence,” software developers saw an opportunity in at least two areas: (1) to assist companies to “scour files and corporate e-mails for evidence and insights into company behavior,” and (2) to assist law firms who conduct forensic examination of a business client’s files in anticipation of litigation.41 One company developed e-discovery software that “forensically collects electronic files from across the organization, automatically analyzes the data, and enables investigators to rapidly identify all evidence and suspects involved in a corporate or government investigation.”42

Another company, Cataphora, developed software that has been described as being able to “detect and comment on sentiment” based on an analysis of electronic messages.43 The software looks for “digital anomalies” by recognizing changes in vocabulary or tone within the communications.44 A compelling assertion by the founder of Cataphora to the New York Times included the following comment: “[The software] doesn’t use keywords at all. But it’s a means of showing who leaked information, who’s influential in the organization or when a sensitive document like an SEC filing is being edited an unusual number of times, or an unusual number of ways.”45

Additional revelations about the Cataphora program, and that of similar software developers, should give pause to any corporate director with questionable communications or motives. These state-of-the-art programs filter documents through a large web of word and phrase definitions. So “[a] user who types ‘dog’ will also find documents that mention ‘man’s best friend’ and even the notion of a ‘walk.’”46 Cataphora uses this tool to detect a person’s activities and interactions to

---

41. *Id.* (emphasis added).
42. See *id.* (quoting CLEARWELL, http://www.clearwellsystems.com/ (last visited Dec. 28, 2011)).
43. See *id.*
44. See *id.*
46. *Id.*
ascertain “who did what when, and who talks to whom . . . [so as to] visualize chains of events,” be it by e-mail, instant messages, telephone calls, or other electronic media.47

The Cataphora founder admits that capturing the “digital anomalies” is exactly the type of behavior “white-collar criminals often create in trying to hide their activities.”48 As described further:

For example, it finds “call me” moments—those incidents when an employee decides to hide a particular action by having a private conversation. This usually involves switching media, perhaps from an e-mail conversation to instant messaging, telephone or even a face-to-face encounter . . . it’s a means of showing who leaked information, who’s influential in the organization or when a sensitive document like an S.E.C. filing is being edited an unusual number of times, or an unusual number of ways, by an unusual type or number of people.49

Specific tools have been developed to recognize sentiment or behavioral shifts. Cataphora’s software can examine e-mails to detect “whether a person is positive or negative, or what the company calls ‘loud talking’—unusual emphasis that might give hints that a document is about a stressful situation.”50 Subtle changes in the style of an e-mail message, such as from casual to atypically formal, are also detected and can “raise a red flag about illegal activity.”51 In the words of Cataphora’s Chief Technology Officer, “You tend to split a lot fewer infinitives when you think the F.B.I. might be reading your mail.”52

Shareholders claiming a director breached his fiduciary duties would likely retain a forensic firm with Cataphora’s capabilities to examine each and every e-mail, telephone call, instant message, or other electronically stored communications for digital anomalies, changes in tone and style (including formal to informal), atypical grammatical variations, or other indicia of stress in those communications. A long-standing director may have hundreds of thousands of such messages, and an entire board may have millions of communications. Needless to say, the director’s every word would be scrutinized. A computer would seem to be the only “person” able to sift through the information at a reasonable cost on a timely basis during litigation.

One recent case illustrated the practical reality that in litigation, computer generated forensics is the only way to go. “Another e-discov-

47. See id.
48. See id.
49. See id.
50. See id.
51. See id.
52. See id.
ery company in Silicon Valley, Clearwell, has developed software that analyzes documents to find concepts rather than specific keywords, shortening the time required to locate relevant material in litigation." During 2010, Clearwell developed a visual presentation of general concepts based on electronic documents. The law firm that hired Clearwell for litigation was able to analyze, sort, and search a half-million documents within the one-week period imposed by the court. In one day, over 3,000 “relevant” documents were identified, allowing one attorney to “do work that might have once required hundreds.”

If a director or the entire board is facing a shareholder suit for breach of fiduciary duties over a period of years, there will necessarily be volumes of electronically stored information (“ESI”) to be analyzed. Competent counsel will likely be aware of the forensic possibilities. If significant economic damages are at stake, the director(s) should expect the shareholders to use these sophisticated tools. Seemingly, defendants have little choice but to ante-up, engage in the forensic arms war, or face defeat, if for no other reason, from the inability to refute the computer-generated findings of plaintiffs’ forensic experts at a reasonable expense and on a timely basis during discovery.

Defense counsel may attempt to exclude such provocative forensic evidence as not being part of a reliable industry or science. To refute such claims, plaintiffs can cite firms like Cataphora, which has Fortune 500 companies, 100 law firms, and federal agencies as customers. Thus, any court inclined to believe that the forensic analytics requires human judgment must face a growing body of work to the contrary. Identifying and measuring a person’s sentiment is certainly commonly regarded as a judgment call. Cataphora’s impressive client list, however, seems to indicate highly sophisticated entities and agencies have already placed enough credence in this artificial evidence to pay to create it.

E. PREDICTIVE ANALYTICS

The use of artificial intelligence to predict human behavior is a developing part of forensic analytics. Within banking and telecommunications, there is a dramatic increase in the demand for algorithms and computer models, sometimes with hundreds operating simultaneously. These complex systems can ascertain when a customer is

53. See id.
54. See id.
55. See id.
56. Castelluccio, supra note 30, at 68.
57. Eric Barkin, CRM + Predictive Analysis: Why It All Adds Up, CRM Mag., May 2011, at 20-21. Algorithms have been defined as a “mathematical or logical process con-
about to cease using the company’s services. For that application, the software programs incorporate several factors, including “trigger dates” of relevant actions, call logs, wireless browsing histories, and notification of when a customer has called a competitor or viewed the competitor’s website. The banking and telecommunications companies use this information, termed “predictive analytics” (“PA”), to establish a protocol to intervene in hope of retaining the dissatisfied customer.

Consider the potential use of PA in legal controversies. A company may use PA to target employees for termination, which may lead to a wrongful termination suit against the employer. If, conversely, the plaintiff retained a software programmer whose PA tool showed the employee performed tasks consistent with the company’s practices and procedures, the admissibility of such evidence could go to the heart of the substantive issue in the employee’s wrongful termination suit. To the point of this Article, it is conceivable that a PA tool could find that a member of the board of directors, or a committee member appointed by the directors, accessed a competitor’s website or made mobile calls in close proximity to certain key votes in one or both companies, votes that individually may appear benign but in sequence infer a plan adverse to the corporation’s interests. The PA tool could also be used to graphically illustrate trigger dates that show a pattern of behavior adverse to the corporation.

Patterns of behavior are significant because there is not always a bright line or single event that causes a breach of fiduciary duties. One act in isolation, such as a failure to pursue the purchase of a competing business, may be excused as a reasonable use of business judgment. A breach of fiduciary duties is more likely to exist when a director ignores several opportunities to purchase the competitor. One example is when there is a familial relationship between the director and a competitor and extraordinary sharing of sensitive information.

sisting of a series of steps, designed to solve a specific type of problem. BLACK'S LAW DICTIONARY 83 (9th ed. 2009).
58. Barkin, supra note 57, at 20.
59. See id.
60. These predictive analytics are discussed in the context of customer retention management (“CRM”). See id. A protocol has been defined as a “common series of rules, signals and conventions that allow different kinds of computers and applications to communicate over a network.” SCHEINDLIN & CAPRA, supra note 12, at 702.
61. The business judgment rule is the subject of voluminous legal literature among courts and academus. See HAMILTON ET AL., supra note 38, at 653 (providing a list of law review articles discussing the business judgment rule). Similarly, section 8.31(a) of the Model Business Corporation Act provides a safe harbor from personal liability when a director is acting in a manner reasonably appropriate under the circumstances. MODEL BUS. CORP. ACT § 8.31(a)(2)(ii)(B) (2005). In this author’s view, as facts change so should the reasonable expectations.
occurs as a result. The ability to correlate call logs, wireless browsing histories, and communications with those family members who prevented the director from purchasing the competitor company can be major factual points in a breach of fiduciary duties claim against the director.

PA tools have already been successfully used in other business circumstances. One PA tool analyzed various demographics of current customers to determine when the customer could not afford a particular plan, signaling when the company should offer a less expensive plan. The PA tool allowed for customer retention worth nearly $40 million annually. Harrah's Entertainment, a gambling conglomerate of more than forty casinos, has been using PA tools for over five years. Harrah's system tracks ten million customers and vast amounts of customer transactions within Harrah's resorts. The customer's behaviors are then used in deciding whether to make additional offers of Harrah services as part of its Total Rewards program or cease marketing to those individuals. One Harrah executive bluntly described the value of its PA tools: "Really it's about understanding which customers are performing worse than others."

Quite conceivably, a company may also use a PA tool to determine whether certain directors are "performing worse than others." The predictive analytic program would gather a wide array of transactional data about its directors, including but not limited to demographic data and extra-office activities such as where they eat, shop, vacation, or gamble from electronically stored information ("ESI"). The corporation could then use the aggregate information to decide whether a director is using judgment or behaving antithetical to the corporation's best interests. Shareholders with access to that same information could then have a basis for requesting the ouster of the director, or the board, if the articles of incorporation so allow, even if a current breach was not evident.

Shareholder access could also give rise to a plausible claim that the director was already breaching fiduciary duties. Even if the company's own PA tool was deemed to be solely predictive, plaintiffs would still have foundational data for their own retained software developer. Plaintiff's forensic expert could then use existing corporate information as a springboard to establish an actual breach indeed occurred.

---

63. See id.
64. See id.
65. See id.
66. See id.
PA has also been used to define and target prospective customers from the vast social media networks. The sources of a computer user's behavioral information are well established in social network profiles, posts, click histories, and usage logs. The PA tool can be used to "discover links among people, organizations, businesses that would otherwise escape the . . . attention of the users." More specifically, this information is used to establish "multifaceted . . . patterns of cooperation and collusion, coalition and co-dependency, influence and deference, and affiliation and isolation among and within groups."

These multiple communication technologies used by corporate directors are within the scope of forensic investigation. Social network data has been compiled and sifted by software developers as they create customized algorithms ("Algos"). The Algos are increasingly used to measure public sentiment. One such Algo used information from Twitter and correlated it with the Dow Jones Industrial Average. Forensic software also analyzes cookies within a smart phone to discover Internet behavior (user's searches, etc.) to help law enforcement with event timelines, Internet usage, habits, and variances from those habits.

67. The commentator first notes that Facebook and Twitter have amassed an enormous user base far beyond opt-in business models. See id. Data mining those social networks is fertile ground for more behavioral analytics.

68. See id.

69. See id.

70. See id.

71. Algos in this context are computer tools that scan social media and other online sources "to predict market movements." Social Media Algos Expected to Multiply, WALL STREET LETTER, Apr. 4, 2011, at 5, http://www.wallstreetletter.com/writeable/custom_uploads/de288d85f3441b5c3f3c8ff9495c4e4c.pdf.

72. Id.

73. One article about Google Analytics provided the following:

Research analysts at CCL-Forensics have forensically recovered vital Internet history data from "cookies" stored within a smartphone, which would not have been retrieved and interpreted using standard forensic tools.

In particular, cookies placed by the Google Analytics service yielded crucial evidence.

Using a number of internally-developed tools, the research and development team retrieved valuable data from more than 1000 cookies.

The data contains information about the domain which placed the cookies, and the ‘value’ of the cookie itself. This ‘value,’ for cookies placed by Google Analytics, can yield timestamps, number of visits, and crucially, referral information.

This means that the digital analyst can see details not only about the site which had been visited, but how the user got there. Where the user arrived at the site via a search engine, this can also include the search terms which led them to that page; this data may not exist anywhere else on the phone.

With this evidence parsed, CCL-Forensics was able to produce a timeline for the law enforcement agency in question, demonstrating with much greater clarity the suspect's Internet usage—and crucially, the evidence of intent showing how the page was arrived at.
The relevance of PA from social media or smart phone usage to this Article is that companies can track social network usage of its directors. Directors are likely to have smart phones provided by the corporation. The company can retrieve and then opine about whether a director's activities indicate patterns of collusion adverse to the company's interests. What is worse for the director is that such damaging information would be self-inflicted and/or self-incriminating. The director would likely establish his own profile, author his own posts, decide when to click on certain websites, and choose to make clandestine calls or web-based searches. As noted above, Algos that correlate wholly legitimate electronic searches of the stock market with other information are already being developed to ascertain the user's sentiments. The customization of linkages to establish director collusion patterns appears, therefore, to be within the scope of existing software technology.

As applied in this Article, a director may make a stock market transaction that unbeknownst to him is being correlated with other information to determine his sentiment for or against the company. Indeed the question of whether mutual fund proxy statements are predictive of responsible decision-making has already arisen.74

The company or a group of shareholders suspecting foul play by a director may potentially use such PA to track the unsuspecting director. Obviously, a director who tweets self-identified naked photos or clicks on websites involving human trafficking or child pornography is subject to potential personal liability. Less obvious, but still a potential source of director removal, are behaviors antithetical to the company's culture. A mutual fund proxy statement authored by the directors or a particular director may be legal on its face but could nonetheless be part of a scheme detected by forensic investigation. All of these consequences are more easily discovered through use of the aforementioned forensic tools that were previously unavailable or underutilized.

F. E-MAIL ANALYTICS

The Enron Corpus was also the testing ground for a linear algebra model that identifies and analyzes asymmetric relationships among

---


computer users based on the exchange of e-mails.\textsuperscript{75} The model is termed DEDICOM.\textsuperscript{76} As forensic tools find irregularities within the exchange of e-mails among board members and outside competitors, or with third parties not in the company's interests, exposure of those exchanges increases as does the potential for breach of fiduciary claims against those directors using the firm's e-mail system.

The United States government has research agencies that also advance the use of artificial intelligence and software-based forensic analytics. The Air Force Institute of Technology concluded that e-mails could be data-mined to discern employee's interests. It conducted such research to better ascertain whether individuals with clandestine interests had the potential to be insider threats to the military.\textsuperscript{77} If we replace "military clandestine insider threats" with "corporate insider threats," we have fiduciary duty actions against corporate directors. The research and technology appears applicable to both.

G. CONTEXTUAL FORENSIC EVIDENCE IN LITIGATION

The legal field has already begun grappling with how to incorporate forensic software programs during federal civil procedure confabs. The Duke Conference of the Federal Civil Rules Advisory Committee convened in May 2010 amid calls for uniform e-discovery rules.\textsuperscript{78} The Committee noted that computer algorithms ("Algos") have increasing use for "clustering, predictive coding, initial document culling, and other search technologies."\textsuperscript{79} Predictive coding is another label for software attempts to use electronic information to judge human behavior. This technique was contemplated, if not directly encountered, in civil litigation.\textsuperscript{80}

Other evidence of recognized forensic analytics is found within a study of litigated issues in e-discovery.\textsuperscript{81} From among the eighty-four most significant e-discovery cases during 2010, the study analyzed the frequency with which certain categories of e-discovery issues were ad-
dressed. In seventeen percent of the cases, procedural issues involving “search protocol” were addressed, and another eight percent dealt with broader “computer forensics protocols and forensic experts.”

Thus, among the cases that involved significant e-discovery issues, one of every four concerned whether the software program, with its algorithms, was sufficiently reliable for admissibility in litigation. If e-discovery issues become hotly contested that often, it is now likely to be part of the standard checklist of any competent counsel’s arsenal of discovery tactics. It appears, therefore, that forensic evidence is already as much a part of litigation as e-discovery itself. Accordingly, the use of this type of analytics and its implications must be incorporated into the law, even if it is to only define when forensic analytics is unreliable or inadmissible. This Article has already provided several illustrations on how forensic tools could be part of shareholder suits against directors. Competent counsel for shareholders would just as readily retain forensic experts with respective software programs when such a serious issue as fiduciary duties hangs in the balance.

Again, these are not abstract firm experiments and anecdotal studies. It is the type of information plaintiff’s counsel is likely to use to establish the science and reliability of its forensic analysis for use in litigation. If there is litigation, counsel for a defendant business should attempt to keep those software-developed documents and any related damaging testimony from seeing the light of day in court. As this Article will discuss below, the more a forensic examination is considered to be “science” or “skill,” the greater the opportunity to admit expert testimony, related documentary evidence, and testing methodologies.

If these software programs, as tested through the Enron Corpus, are considered a reliable basis for finding fraud or other inappropriate or illegal behavior, there is a consequence far beyond the costs of discovery. The cost of personal liability to corporate boards of directors is an issue very much in play. And speaking of play, the very real game of using a computer to mimic human reasoning skills and compete against humans has already occurred—it was a historic battle between a computer named Watson and the intellectually gifted among our species.83

82. See id.

83. Watson was not the first computer being to emerge from the imagination of the human species. Before Watson was Hal, the better-than-human intelligent computer in 2001: A Space Odyssey, by Arthur C. Clarke and Stanley Kubrick. See Arthur C. Clarke, 2001: A SPACE ODYSSEY (1968) (providing the book version of the story); see also 2001: A SPACE ODYSSEY (Metro-Goldwyn-Mayer 1968) (providing the movie version of the story).
It does not take much imagination to envision Watson's brain with Cataphora-like forensic software, which is used to match wits with defense counsel. Imagine Watson claiming in monotone, "The e-mails of director X of this corporation show digital anomalies from June 2, 2006, through August 27, 2011, on 1,149 entry dates, based on the previously tested Algo sequences. Those anomalies evidence fraud." Watson may have reams of supporting evidence and backup tapes that are literally miles high. Defense counsel would of course attempt to refute the evidence against the director. As one commentator feared, however, only Watson committed to memory the Enron Corpus and testing methodology to assure the findings' reliability. A director and defense counsel without a Watson of their own would be at serious risk of being defenseless.

III. ISSUES OF PROCEDURE AND ADMISSIBILITY: LITIGATION HOLD AND SEARCH PROTOCOL

As noted above, there is no practical value in discussing the impact of forensically derived evidence against corporate directors if the forensic evidence is categorically inadmissible. Corporate counsel would simply file a motion for summary judgment and the case would disappear. The forensic evidence would therefore need to be relevant and admissible evidence as gained through discovery.

Forensic evidence is part of electronically stored information ("ESI"). The courts have considered ESI in litigation so often in the past few decades that e-discovery is its own sub-titled jurisprudence. Within e-discovery there are several steps, with a threshold issue of when ESI must be preserved. The general rule is that ESI preservation should start when an entity has reasonable knowledge of pending litigation. As stated in Treppel v. Biovail Corp., "The obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation." Since the obligation is an objective "should have known" rather than a subjective standard, the corporate client has no safe harbor by pleading ignorance to relevant facts known to other corporate officers. Additionally, a director has no excuse from his or her obligation if he or she had reasonable access to customary communication regarding

84. Castelluccio, supra note 30, at 68.
85. See Scheindlin, supra note 9, at 2 (providing an extensive discussion of e-discovery).
such information. This constructive knowledge leads to an affirmative obligation to preserve, i.e. to place a “litigation hold” on potentially relevant documents, including ESI. 88

Of particular relevance to this Article is the next step. As in Treppel, the parties may not agree on what ESI must be preserved. After motions to expand or narrow the scope, the court may enter an order clarifying three obligations on the party producing ESI: (1) that the defendant corporation conducts a search, (2) that the search explains its “search protocol,” and (3) that the defendant produces responsive documents consistent with that search protocol. 89

In Treppel, the parties did not agree on a particular search protocol. The court noted that the plaintiff refused to stipulate to an appropriate protocol, leaving the defendant with the sole risk of responsive production. 90 The important point is that regardless of whether the parties agree or argue about the protocol, the court is likely to establish one. If the plaintiff convinces the court to require a protocol that includes behavioral searches, the defendant is in a difficult position. The search may reveal potentially incriminating evidence about the corporation’s own employees, officers, and directors. According to the Treppel test, the failure to follow that protocol and produce documents could result in significant sanctions or other remedies. 91 The defendant corporation is caught in the legally uncomfortable position of having to preserve the very evidence that could damage its directors’ defenses.

The consequences of production under a plaintiff’s protocol could be damaging in various respects. As discussed above, a software programmer may develop a forensic analytics program designed to not only recover raw data, but also organize it in such a manner that it suggests predictive behavior. The plaintiff may retain the programmer for purposes of this litigation. If the defendant corporation has no such programmer, the court may be more convinced by the party with

88. In one court’s words, “Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a ‘litigation hold’ to ensure the preservation of relevant documents.” Zubulake v. UBS Warburg LLC (Zubulake IV), 220 F.R.D. 212, 218 (S.D.N.Y. 2003).
90. Understandably, the plaintiff may have had a war mentality and refused to let defendant “off the hook” or make life easier.
91. Those remedies include significant monetary sanctions, adverse inferences in jury instructions against the nonproducing party, and even default judgments against that party. See Zubulake IV, 220 F.R.D. at 222; see also Gutman v. Klein, No. 03 Civ. 1570(BMC), 2008 WL 5084182 (E.D.N.Y. Dec. 2, 2008). Thus, the failure to comply is not a viable option.
the apparent expertise to develop the protocol. In this case, the plaintiff would have the decided advantage.

The possibility of a plaintiff retaining an expert with a prevailing protocol over a defendant corporation is not remote—indeed, many corporate employers may be at a disadvantage. One e-discovery study of “461 IT professionals and in-house counsel from the United States and Britain” concluded that only forty-six percent of U.S. companies and forty-one percent of British companies “have a policy addressing e-discovery readiness,” indicating they face these issues instead on a case-by-case basis. Ad hoc handling of these issues is likely to also give rise to a lack of forensic software experts already steeped in company culture and institutional knowledge. Of equal concern, less than half of the surveyed companies updated their policies to include new technologies, though policies should be updated no less than twice a year. These failures make such companies vulnerable to losing the arms race for an accepted forensic protocol.

Consider the ramifications of a plaintiff protocol on a defendant’s future potential admissions, inferences, or disadvantages in proofs. Assume the above hypothetical where the company had the repeated opportunity to purchase a competitor. Assume as well there is compelling evidence that the purchase would significantly increase the company’s market share, profitability, and share value. One particular director is the most powerful and influential and has the swing vote among the board members. The director purposefully and repeatedly votes against the purchase.

A group of shareholders alleges that the director has close relatives on the competitor’s board resulting in a conflict of interest, has engaged in self-dealing, and has personally profited from the separation of companies. The plaintiff shareholders may only have thin, unsubstantiated allegations at the commencement of litigation. If, however, their forensic expert establishes a protocol requiring the director and the corporation to produce information showing the director’s communications with or about the competitor, organized and presented according to the plaintiffs protocol, then digital anomalies and links in communications that evidence clandestine insider threats between the defendant director and the relatives in the competing corporation could be almost assured if the jury believes the forensic evidence. In turn, such information would be prime evidence of the director’s self-dealing and conflicts of interest in breach of his fiduciary duties.

93. Id.
This very early stage of discovery may increasingly become a more intense battleground than exists in current practice. The battle is over whose protocol will be used. The issue can be hotly contested because, if a well-armed plaintiff wins the battle, she may also win the war.

There are a host of additional evidentiary issues, many of which are already subject to substantial scholarly discussion. One primary issue is whether a forensic programmer and analyst could qualify as an expert witness. Federal Rule of Evidence ("FRE") 702 governs the admissibility of testimony based on "scientific, technical, or other specialized knowledge." Since we are dealing with cutting edge forensics, it is significant that the Advisory Committee's Note explicitly recommends a broad interpretation of the types of knowledge experts can use in developing an opinion. In the words of the Advisory Committee ("Committee"), "The fields of knowledge which may be drawn upon are not limited merely to the 'scientific' and 'technical' but extend to all 'specialized' knowledge. Similarly, the expert is viewed, not in a narrow sense, but as a person qualified by 'knowledge, skill, experience, training, or education.' The Committee further rejected confining experts "in the strictest sense of the word" to traditional occupations as "physicians, physicists, and architects." Specifically included in its example is the "large group" of "skilled" witnesses. Examples included "landowners testifying to land values."

This interpretative language gives all the more credence to including forensic analysts with behavioral conclusions from mathematical algorithms as expert witnesses. While they certainly could already be classified as having technical knowledge, they more certainly can be offered as having training, education, and skill in developing software designed to analyze the ESI users' actions. The emerging field that draws behavioral conclusions appears comfortably within the "specialized" knowledge now allowed under FRE 702.

94. See generally Scheindlin & Capra, supra note 12, at 517-61.
95. Fed. R. Evid. 702.
97. See id.
98. See id.
99. See id. No discussion of scientific expert testimony is complete, however, without including the landmark case of Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579 (1993), and its progeny. While Daubert appears to have a rather restrictive five-part test for admissibility, several courts and commentators opine that Daubert is more the exception than the rule and that the current federal rules of evidence were drafted in reaction to the restrictiveness to broaden the parameters of scientifically-based expert testimony. See, e.g., Paul F. Rothstein, Federal Rules of Evidence 908 (Mark L. Lupisella et al. eds., 3d ed. 2010); see also Kumho Tire Co., Ltd. v. Carmichael, 526 U.S. 137, 149-50 (1999); Kannankeril v. Terminix Int'l Inc., 128 F.3d 802, 806, 809 (3d Cir. 1997).
The obvious companion of forensic expert testimony is the written and technical report relied upon by an expert. FRE 703 explicitly allows facts or data that is "of a type reasonably relied upon by experts in the particular field." An underlying goal of both FRE 702 and 703 is to prevent unreliable and untested information from reaching a jury—be it in the form of testimony or data used to support the testimony. Arguably, since FRE 702 has a broad view of the "knowledge" requirement for expert testimony, including those with non-traditional "skills," the scope of a "particular field" under FRE 703 is likewise broad. Stated differently, if forensic programmers of behavior analytics are part of the group with "skills" or "specialized" knowledge sufficient to provide expert testimony, it would be consistent to also broadly define "field" for admissibility of facts and data they can use to support that testimony.

Evidentiary rules for authentication of documents likewise appear to be broad enough to include forensic analytics that use mathematical algorithms and models. FRE 901(b)(9) is frequently used to authenticate computer-generated information. A process or system, such as a forensic program, must meet two foundational requirements for admissibility. First, it must be described. Second, it must be able to produce an accurate result. These points must be established by the testimony of someone with knowledge or control of the computer program and who is sufficiently familiar with its operation. A body of law has already developed, though still evolving, to authenticate computer-generated evidence, including digital animation, simulations, and computerized models. One commentator noted that computer-generated evidence has been used "to construct hypothetical markets in an antitrust claim for purposes of illustrating anticompetitive behavior." If forensic evidence can be used in the complex arena of antitrust law, there should be equal access for admissibility in general business organization issues involving directors' fiduciary duties.

Beyond evidentiary rules, none of the reviewed cases or commentary attempt to categorically preclude forensic analytics as evidence. Thus, the cautions to corporate directors suggested above appear fully relevant and worthy of consideration.

100. Fed. R. Evid. 703.
101. See Fed. R. Evid. 702-03.
102. Algos are computer tools that scan social media and other online sources to make predictions. See Social Media Algos Expected to Multiply, supra note 71.
103. See Fed. R. Evid. 901(b)(9).
105. Id. at 354.
IV. SUBSTANTIVE CLAIMS AGAINST DIRECTORS FOR BREACHES OF FIDUCIARY DUTIES

A. Plaintiffs’ Quiver of Claims—A Wide Array of Theories and Causes of Action

Directors occupy a position of trust and confidence to act in the corporation’s interests.\(^\text{106}\) As such they are fiduciaries with affirmative duties to act or avoid acting against those interests.\(^\text{107}\) Broadly stated, directors have a duty of care and a duty of loyalty.\(^\text{108}\) There is, however, a rather complex web of duties, due in part to the interrelationship between case law and statutory provisions within various states. At times, state legislatures react to case law, and other times, case law reacts to statutory provisions. Those dynamics give rise to some variance from state to state. Yet, a substantial majority of states follow the Model Business Corporation Act ("MBCA").\(^\text{109}\) Delaware’s corporate statutes are also viewed as an influential guidepost, so this Article will examine principal provisions from both the MBCA and Delaware’s business statutes and some of the interpretive case law.

Another factor that adds to the complexity of defining fiduciary duties is judicial interpretations of good faith and the business judgment rule.\(^\text{110}\) Both are safe harbors against a director’s personal liability. As noted above, the business judgment rule has been subject to extensive discussion, and though the MBCA requires good faith for directors, it remains an undefined term.\(^\text{111}\) Courts have viewed the doctrines as being based in common law, sufficiently independent from a state’s business statutes. Courts, for example, have linked a lack of good faith to defeat the corporation’s attempt to absolve itself of liability through use of the business judgment rule.\(^\text{112}\) This Article, however, will view the concepts like a defendant director—as separate counts in a complaint.

\(^{107}\) The Model Business Corporation Act ("MBCA") provides that directors must act "in good faith" and "in a manner the director reasonably believes to be in the best interests of the corporation." MODEL BUS. CORP. ACT § 8.30(a) (2005).
\(^{108}\) The duty of care is principally found in section 8.30 of the MBCA. See MODEL BUS. CORP. ACT § 8.30. The duty of loyalty is principally lodged at sections 8.60 and 8.61 of the MBCA. See MODEL BUS. CORP. ACT §§ 8.60, 8.61. There is a substantial body of case law developed before and after such provisions that give rise to multiple arrows in the plaintiff’s quiver of claims.
\(^{109}\) According to one source, three-fourths of the states have enacted the MBCA’s standard duty of care. See WILLIAM E. KNEPPER & DAN A. BAILEY, LIABILITY OF CORPORATE OFFICERS AND DIRECTORS 3-3 (8th ed. 2010).
\(^{110}\) See supra note 61 and accompanying text.
\(^{111}\) See supra note 61 and accompanying text; see also infra note 126 and accompanying text.
Two other factors add to the complex web of a director's fiduciary duties. First, there are independent sources of liability within separate bodies of laws and subjects that could give rise to fiduciary duty claims. Second, and perhaps more importantly, statutory provisions have subsections that courts have cited so that several different fact patterns could give rise to breach of fiduciary duty claims. And as noted above, common law stands apart from state statutes. The list of some primary characterizations of fiduciary breaches is noted below, presumably any one of which a court may find sufficient to hold a director or the corporation liable.

<table>
<thead>
<tr>
<th>CLAIM</th>
<th>SOURCE OF AUTHORITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure to discharge duties in good faith</td>
<td>Duty of Care—Model Bus. Corp. Act § 8.30(a)</td>
</tr>
<tr>
<td>Failure to discharge duties using reasonable belief in best interests of the corporation</td>
<td>Duty of Care—Model Bus. Corp. Act § 8.30(a)</td>
</tr>
<tr>
<td>Inadequate disclosure of material information needed for decision-making or oversight functions</td>
<td>Duty of Care—Model Bus. Corp. Act § 8.30(c)</td>
</tr>
<tr>
<td>Reliance on information knowing such reliance is unwarranted</td>
<td>Duty of Care—Model Bus. Corp. Act § 8.30(d)</td>
</tr>
<tr>
<td>Delegating to and reliance on others who the director cannot reasonably believe have the &quot;skills or expertise&quot; to be reliable and competent</td>
<td>Duty of Care—Model Bus. Corp. Act § 8.30(d)-(f)</td>
</tr>
<tr>
<td>Reliance on information, opinions, or reports of others who the director cannot reasonably believe is reliable and competent</td>
<td>Duty of Care—Model Bus. Corp. Act § 8.30(e)-(f)</td>
</tr>
<tr>
<td>Conflict of interest in transactions when the director or a related person had a material financial interest that was unfair to the corporation without disclosing the existence and nature of the conflict and without ratification by disinterested directors of the corporation</td>
<td>Duty of Loyalty—Model Bus. Corp. Act § 8.60</td>
</tr>
</tbody>
</table>

113. For example, there are civil liability provisions in the Securities Act of 1933 involving the sale of unregistered securities, material misstatements or omissions in a registration statement, or misleading statements in the sale of securities. See Securities Act of 1933, ch. 38, 48 Stat. 74 (codified as amended at 15 U.S.C. §§ 77a-77aa (2010)). There are also federal antifraud provisions, insider trading rules, and personal liability for directors under federal environmental laws.

114. Under the MBCA, a director could have a separate basis for personal liability for self-dealing, conflict-of-interest transactions, than when voting for unauthorized distributions to shareholders or acting in bad faith or not reasonably within the best interests of the corporation. Model Bus. Corp. Act §§ 8.30, 8.33, 8.60.

115. Violations of securities statutes in federal and state law could obviously bring potential companion claims for investigation using forensic tools but are beyond the scope of this Article.

116. The following table provides a list of claims and the corresponding section of the MBCA or case law where such claim would arise. See Model Bus. Corp. Act §§ 8.30, 8.60; see also infra notes 118-125 and accompanying text. See generally Knepper & Bailey, supra note 109, at 2-1 to 4-56.
<table>
<thead>
<tr>
<th>Failure to act in good faith (i.e., acting with a purpose other than for the best interests of the corporation)</th>
<th>Duty of Loyalty—Case Law117</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acting arbitrarily or for laudable purposes instead of the best interests of the corporation</td>
<td>Duty of Loyalty—Case Law118</td>
</tr>
<tr>
<td>Appropriating a “corporate opportunity”</td>
<td>Duty of Loyalty—Case Law119</td>
</tr>
<tr>
<td>Failure to fully disclose “material” facts from the view of a reasonable shareholder</td>
<td>Duty of Fair Dealing—Case Law120</td>
</tr>
<tr>
<td>Trading shares based on “confidential information acquired through [the director’s] fiduciary position”</td>
<td>Duty of Loyalty—Case Law121</td>
</tr>
<tr>
<td>Taking unfair advantage of corporate procedures, program, or operations to maintain control against the interests of the corporation and its shareholders</td>
<td>Duty of Loyalty—Case Law122</td>
</tr>
</tbody>
</table>

117. See In re Walt Disney Co. Derivative Litig., 906 A.2d 27, 67-68 (Del. 2006); see also Stone v. Ritter, 911 A.2d 362 (Del. 2006). See generally Knepper & Bailey, supra note 109, at 4-4 (providing a line of cases regarding the duty of loyalty). It is worth noting that the duty of loyalty is not confined to just conflict of interest transactions since a failure to implement a reporting system or oversee operations is also a basis for breach of the duty of loyalty. See Stone, 911 A.2d at 370. And while Stone clarifies that a lack of good faith is not an independent basis for liability, it also notes that good faith is required as part of the duty of loyalty as a subsidiary element of that duty. Id.; see Knepper & Bailey, supra note 109, at 4-3. Other cases broadly state the same fundamental requirement of directors to refrain from acting in a way that subrogates the interests of the corporation to the director's personal interests, though the bad faith label was not attached. See In re Allegheny Int'l, Inc., 954 F.2d 167, 180 (3d Cir. 1992).


119. Generally, courts have opined that if a corporation has the financial resources and legitimate expectancy of an opportunity, a director cannot divert that opportunity to himself, particularly if the opportunity only came to the director through his position or his use of corporate assets. See, e.g., In re Safety Int'l, Inc., 775 F.2d 660, 662 (5th Cir. 1985).

120. See Loudon v. Archer-Daniels-Midland Co., 700 A.2d 135, 143 (Del. 1997); see also Knepper & Bailey, supra note 109, at 4-8 to 4-10.1 (providing a line of cases supporting the duty of disclosure). The duty of fair dealing is generally attributed to the American Law Institute and is regarded as very similar to the conflict of interest prohibitions, both of which involve the self-interested director in a transaction affecting the corporation. See Knepper & Bailey, supra note 109, at 4-7.

121. McCall v. Scott, 239 F.3d 808, 824 (6th Cir. 2001); see also Polin v. Conductron Corp., 552 F.2d 797, 811 (8th Cir. 1977).

122. See Bennett v. Breuil Petrol. Corp., 99 A.2d 236 (Del. Ch. 1953). The key element to finding a director took unfair advantage is demonstrating an improper purpose for the director's conduct that is against the interests of the entity. A director's desire to maintain control through the purchase of shares or solicitation of proxies is not itself improper or a breach of fiduciary duty. See Rosenfeld v. Fairchild Engine & Airplane Corp., 130 N.E.2d 610 (N.Y. 1955).
In selling controlling shares, failing to sell shares in a manner that is inherently fair to minority shareholders of the corporation

| Duty of Loyalty/Inherent Fairness Test—Case Law 123 |
| Selling shares and transferring control to those who may “loot” the corporation | Duty of Loyalty—Case Law 124 |

These claims are not available in all jurisdictions, but nonetheless provide a range of potential challenges to a director's actions within a general breach of fiduciary duty claim. This attempt to present a comprehensive view of fiduciary duties is important in the context of this Article because only with such a view is the reader aware of the multitude of ways electronically stored information (“ESI”) can be collected and manipulated through the forensic tools noted above to pose liability risks for corporate directors.

Many of the cases are shareholder derivative suits. This Article examines those cases because a director’s failures can be revealed from the recovery of voluminous ESI. Those failures may have adverse consequences to the corporation, and therefore be a source for director liability.125

There are several defenses available to directors.126 This Article, however, examines the risks of liability in light of forensic ESI analy-

123. The inherent fairness test incorporates the notion of fair dealing such that the duty of loyalty is violated if the director uses inside information and his own strategically advantageous position to personally benefit to the detriment of shareholders or otherwise uses his power to do “indirectly through the corporation what he could not do directly.” See Jones v. H. F. Ahmanson & Co., 460 P.2d 464, 471 (Cal. 1969). In Jones, minority shareholders alleged that the majority shareholders created a new entity and then transferred controlling interests of the original corporation to that new entity, thereby establishing a new public market for the new entity while consequently causing the minority shares in the original entity to become unmarketable. See Jones, 460 P.2d at 469.

124. There are a line of “looting cases” that imposes a duty to reasonably investigate the motives and intent of the purchasers prior to sale and transfer. See Doleman v. Meiji Mut. Life Ins. Co., 727 F.2d 1480, 1483-84 (9th Cir. 1984) (providing a list of citations to “looting cases”). If a director is a majority shareholder, the duty to reasonably investigate the motives and intent of purchasers runs from the director to the corporation and also minority shareholders. See Harris v. Carter, 582 A.2d 222, 234-35 (Del. Ch. 1990).

125. The other apparent source may be a former employee who files a wrongful termination suit against not only the corporation, but also its directors.

126. For example, MBCA conflict-of-interest provisions contain substantial procedural challenges to plaintiffs. No damages or equity relief can be granted if the transaction is authorized by a majority of qualified directors. MODEL BUS. CORP. ACT § 8.62. Nor will damages or equity relief be granted if the transactions falls outside of the detailed definition of a “director's conflicting interest transaction.” MODEL BUS. CORP. ACT §§ 8.60, 8.61(a). Nor will damages or equity relief be granted if there is ratification by a majority of the shareholders to transaction that qualifies as a conflicting interest transaction under the statute. MODEL BUS. CORP. ACT § 8.63(a). Another important defense is the business judgment rule (“BJR”), which precludes judicial interference with good faith judgment calls of directors, even if the decisions appear unwise, so long as there is no
sis without attempting to determine in each type of case, a prevailing party in litigation. The risks are shown primarily from the plaintiff’s claims. Accordingly, the numerous director defenses are not analyzed.

It is important to note, however, that the majority of statutory defenses under the MBCA do not defeat unreasonable actions by directors. Many provisions require that the director act reasonably in the best interests of the corporation, with actions justified when the director acts consistent with a person in a like position, or when the director relies on opinions of others that she reasonably believes are reliable and competent. 127 Thus, a director’s risks are still very high if a plaintiff uses ESI to establish unreasonable actions or acts of omission by the director.

B. **The Defendants**

Directors are generally required, but do not have to be shareholders, unless prescribed by the articles of incorporation or bylaws. 128 There is no general statutory prohibition against a director also being an officer or other executive within the corporation. A director, therefore, may wear many hats. There is also no general statutory prohibition against a director of one company having a financial interest or management role in a related corporation, though articles or bylaws could establish those limitations as part of the position’s qualifications. 129

The Enron prosecutions provide a broad scope of executives potentially subject to civil liability for breach of fiduciary duties. 130 Twelve of the forty-six defendants held the title of Chief Executive Officer,

“abuse of discretion, fraud, bad faith, or illegality.” See, e.g., Int’l Ins. Co. v. Johns, 874 F.2d 1447, 1461 (11th Cir. 1989); In re Oracle Corp. Derivative Litig., 808 A.2d. 1206 (Del. Ch. 2002); Auerback v. Bennett, 393 N.E.2d 994, 1000 (N.Y. 1979). The rule even has a codification in the MBCA designed specifically for shareholder derivative suits, stating such actions shall be dismissed if the directors acted in good faith, after reasonable inquiry, and the suit is “not in the best interests of the corporation.” MODEL Bus. CORP. ACT § 7.44(a). There are several other motions defense counsel can assert to prevent production of documents or testimony, including attorney-client privilege, undue burden, lack of reliability, hearsay, and violations of the federal privacy law for electronic communications. See In re Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606 (E.D. Va. 2008); see also Michele C.S. Lange & Kristin M. Nimsgern, ELECTRONIC EVIDENCE AND DISCOVERY: WHAT EVERY LAWYER SHOULD KNOW NOW 274 (2d ed. 2009).

127. See MODEL Bus. CORP. ACT § 8.30(a) (providing the requirement for reasonableness as a director to act in good faith and in the best interests of the corporation); see also id. § 8.30(b) (providing for like person reasonableness in oversight functions); id. § 8.30(f) (providing for reasonable reliance on the opinions or reports of others).

128. See MODEL Bus. CORP. ACT §§ 8.01(a), 8.02 (2005).

129. See id. § 8.02 (allowing the articles of incorporation or bylaws to prescribe qualifications for directors).

130. The Enron litigation primarily involved criminal fraud, but the alleged egregious actions would provide the factual basis for similar civil claims.
Chief Operating Officer, President, Chairman of the Board, Senior Partner, Executive or Senior Vice President, Investment Advisor, Chief Legal Officer, or Vice President for Legal Affairs. Pursuant to the MBCA, a board of directors may establish committees, allowing directors to serve on the committees, unless the corporation's articles of incorporation or bylaws provide otherwise. In the Enron example, the persons holding the titles listed above could also have been directors who are subject to shareholders' breach of fiduciary duty claims.

C. DEFINING THE "DUTY" IN THE DIGITAL WORLD

Generally, the corporate director has a standard of care and fiduciary duty to both the corporation and its shareholders. A primary potential source of conflict between the corporation, its directors, and its shareholders can be explained in terms of a director's pressure to fulfill multiple, sometimes conflicting obligations. Directors are stewards for the corporation's best interests, which often involve increasing financial performance and value for the corporation and its shareholders. Factors that affect a director's performance include the pressure to produce ever-increasing profits and assets, while lowering debt service. The patterns of director behavior are of particular relevance to this Article because identification of those patterns is also at the core of what forensic investigators find and analyze.

In the case of Enron, the core legal issues involved a pattern of accounting and audit failures and misdeeds. Self-interested transactions, cover-ups, and document obfuscation occurred, originating from a common temptation to increase profitability, albeit beyond the bounds of the law. Unless we believe the Enron executives were a breed apart, beamed to earth in error never to return again, the underlying causes of fraud and deceit still lurk amongst us. That is why shareholders still bring breach of fiduciary duty claims against individuals with the same titles as the executives in Enron or other corporations rocked with recent scandals.

132. See MODEL BUS. CORP. ACT § 8.25(a).
133. See MODEL BUS. CORP. ACT § 8.31(a) (2005) (referencing liability to "the corporation or its shareholders"); see also MODEL BUS. CORP. ACT § 8.63(a) (concerning an action by shareholders for a "director's conflict of interest transaction").
135. See id. at 93 (providing a list of results from organizational pressures).
136. See id. at 100 (stating some of the well-documented improprieties that included the abuse of certain "related-party" partnerships to show phenomenal success).
The shareholder plaintiff’s quiver of claims is generically sourced from historical development of cases and statutes in business law jurisprudence. The advent of electronically stored information (“ESI”) has already changed the landscape of corporate litigation. The reasons for updating rules to accommodate ESI have been well stated by advisory committees established to make civil procedural rules to accommodate ESI.\textsuperscript{137} To the thesis of this Article, those same reasons present a need to analyze the impact of ESI, not just for litigation generally but specifically for breach of fiduciary duty actions against directors.

The potential for forensic evidence to assist plaintiffs is apparent. There are many fact situations that could give rise to an assertion that a director breached a fiduciary duty. A director’s actions could place him in one of those situations in ways that would not have been contemplated in a pre-digital world. Put more ominously, consider the various means now available that allow software programmers to use forensic tools to access years of e-mails, cell phone calls, or documents stored on hard drives or remote storage devices, which are beyond the director’s mental capacity to recall. So while the digital age has not altered the sources or definitions of the fiduciary duty, the recovery of information that may establish those violations has. Therein lies the potential for more aggressive actions and the need for heightened awareness of all communications by corporate directors.

D. DATA RECOVERY AND ANALYSIS

Plaintiff’s counsel typically utilize a three-step forensic process, commencing with retention of a forensic expert who develops a strategy to collect and analyze the data, followed by the actual data recovery and analysis, and then the expert report and testimony.\textsuperscript{138} This Article focuses on the data recovery and analysis from which the director’s risks are ascertained.

There are numerous avenues available to a forensic examiner to retrieve a director’s electronically stored information (“ESI”). It is important to note that forensic tools can collect data from virtually any storage device, even files that have been accidentally deleted, corrupted or otherwise modified.\textsuperscript{139} A director, therefore, has no safe harbor in obsolete computer systems discarded by the corporation.

\textsuperscript{137} See supra note 4 and accompanying text. The sheer volume of e-mails and other information, evolved means of sifting data, and the ability to analyze behaviors required special rule amendments.
\textsuperscript{138} See Lange & Nimsgern, supra note 126, at 210-11.
\textsuperscript{139} See Scheindlin & Capra, supra note 12, at 57.
Forensic recovery involves both the retrieval of data and the "imaging" of that data. "Imaging" exists where software provides an exact byte-by-byte duplicate copy of the original data. Importantly, the image also reveals any unused areas and user "overwriting" where old data is replaced with new data during ordinary computer use. The ability through imaging to see unused areas is important because once a director inputs new information, the investigator can see what information was subsequently added and when. This can also be valuable if the director is allegedly attempting to erase incriminating e-mails.

Particularly relevant to this Article is the step after data retrieval—analysis. Forensic investigators can ascertain if the computer evidence has been "tampered with, altered, damaged, or removed." This can be achieved by scanning the hard drives to break password protections or file encryptions. From discovering patterns of password use, individual users may be identified and linked to all types of information in various locations.

Forensic examiners can then perform the following types of analysis:

1. Recreate a specific chain of events or user activity, including all Internet activity and e-mail communications;
2. Search for keywords or key dates;
3. Search for copies of prior drafts of documents;
4. Verify and authenticate dates and times for particular files;
5. Ascertain if a USB jump drive (flash memory stick) has been used with a specific computer;
6. Ascertain if a certain computer program is original or copied from another program through code comparisons; and
7. Gather data that reveals if data was copied to another location or different media type.

The re-creation of a chain of events may be most concerning to a corporate director faced with breach of fiduciary duty claims. Many of the factual scenarios giving rise to such claims involve affirmative
acts of the director. Misappropriation of a corporate opportunity is one such act, and the plaintiffs’ ideal evidence would show a nexus between the director and the opportunity, and that the opportunity was only available through the director’s corporate position or assets. The forensic analysis may show the time and date of meetings between the director and the source of the opportunity. The analytics may also establish that the corporation owned the computer used by the director or that drafts of damaging documents were originally authored by the director and deleted only after notice of the plaintiffs’ action.

Successful plaintiffs then would establish that the corporation could have reasonably desired involvement in the opportunity and the requisite resources. An analysis of traditional patterns of e-mails and communications from the director on other opportunities could be compared and contrasted to the opportunity in question to note any digital anomalies. This type of forensic analytics evidences a chain of events and patterns of conduct that the plaintiffs could pursue to the potential detriment of a defendant director.

E. THE PREEMINENT IMPORTANCE OF METADATA AND UNVEILING ATTEMPTS TO DESTROY EVIDENCE

The ability to discover and analyze computer information often depends on metadata, which is “data about data—the who, what, where, why, and how about a file.”145 Software programs, file systems, and operating systems create and store metadata (e.g. when a file was created, last modified, size of file, etc.).146 Each program or system has unique features within its own metadata that enhance the ability to locate and isolate sources of information.147 As discussed above, metadata is like the computer’s DNA and can be a basis for predictive behavioral analysis as it provides “clues to human behavior.”148

Whenever a computer is used, there is a level of file change and data destruction. The occurrence can be completely innocent. In fact, every time a user boots up a computer several files are accessed and some are modified.149 The storage device within the computer has files, some used and others unused. Every new boot-up of the computer can modify the metadata of the files in new and used space and even temporary cache files. Thus, even by booting-up, the director

145. LANGE & NIMSGER, supra note 126, at 233.
146. See id. Operating systems are the software that other software depends on to make a computer functional. See id. at 232.
147. See id. at 233.
148. See SCHEINDLIN & CAPRA, supra note 12, at 2 n.4.
149. LANGE & NIMSGER, supra note 126, at 220.
gives "clues" regarding the history of his computer usage. This process is part of what is termed "overwriting" of existing files.

Metadata is now established as part of discovery in litigation, including civil cases involving fiduciary duty claims. Courts have explicitly rejected defendants' arguments that "metadata is an inherently not part of an electronic document" and therefore is not to be produced in discovery. A prominent case for this point involved a defendant corporation that resisted production of Microsoft Excel spreadsheets. The defendant explained that it scrubbed the metadata from the spreadsheets so the plaintiffs could not "undelete" or otherwise recover privileged information from the spreadsheets. The court stated that metadata is not directly part of the document since by definition, metadata is "information about a particular data set which describes how, when and by whom it was collected, created, accessed, or modified and how it is formatted, including data demographics such as size, location, storage requirements and media information."

The court emphasized that "metadata is the key to showing the relationships between data" and without metadata, certain data "would have minimal meaning." Accordingly, it held that while not all metadata need be produced in every case, "metadata associated with changes to the spreadsheets, data of changes, identification of those the individuals making the any changes, and other metadata from which [the p]laintiffs could determine the elimination on final versus draft versions of the spreadsheets appeared relevant" and must be disclosed.

Posit the circumstance where a corporate director has compromising information on spreadsheets that shareholders claim reveals his efforts to freeze out shareholders, secretly profit from transactions, or take any other bad faith action. The director faces the probability of not only document disclosure, but also the metadata that will essentially allow a forensic analysis on that very spreadsheet. As described in Williams v. Sprint/United Management Co., the analysis can reveal far more than the information contained within the actual document. All such information can buttress such claims about a director's knowledge or intent to scheme at the corporation's expense.

150. See id.
152. See Williams, 230 F.R.D. at 644-45.
153. Id. at 645.
154. Id. at 646. The court also noted that "[m]ost metadata is generally not visible when a document is printed," but "can be altered intentionally or inadvertently." Id.
155. Id. at 647.
156. Id. at 653.
Another method of data destruction is known as “wiping.” Wiping is cleaning the computer data for a subsequent use (i.e. an IT department wipes a computer to prepare it for sale to a third party or redeployment within the company).\textsuperscript{158} Some forensic experts have made observations that could implicate the director directly, stating, “If it is our experience that individuals attempting to permanently destroy evidence of their activity, such as bad acts, committed on the computer will purchase and run wiping utilities . . . . If run properly, a wiping utility will make the data unrecoverable by commercial computer forensics experts.”\textsuperscript{159}

What the nefarious user may not know is that forensics experts can often still identify the “date, time, and specific program used to conduct the wiping.”\textsuperscript{160} Coupled with other facts, a circumstantial case may still be made against the computer user, here a corporate director.

In \textit{Kucala Enterprises, Ltd. v. Auto Wax Co.},\textsuperscript{161} a forensic expert determined that the night prior to imaging of original files, a wiping utility was used to delete and overwrite more than 12,000 files, and that 3,000 more files were deleted and overwritten three days earlier.\textsuperscript{162} The expert identified the brand name of the wiping utility and claimed that the same product had been used in several other cases where either the plaintiff or defendant destroyed computer evidence in the face of litigation.\textsuperscript{163} There is now a line of cases exposing a party’s attempt to destroy electronically stored information (“ESI”) that is harmful to that party’s case.\textsuperscript{164}

These wiping cases also reveal the creative efforts of an opposing party, authorized by the court, to find alternate means of gathering

\textsuperscript{158.} See \textit{LANGE & NIMSGER, supra} note 126, at 221.
\textsuperscript{159.} See id.
\textsuperscript{160.} See id.
\textsuperscript{161.} No. 02 C 1403, 2003 WL 21230605 (N.D. Ill. May 27, 2003).
\textsuperscript{163.} See \textit{Kucala}, 2003 WL 21230605, at *1-2 (describing, among other things, the name of the wiping utility as “Evidence Eliminator”). Other products are more innocuously labeled such as “Window Washer” and “Cyberscrub,” to name a few. There are other cases where a party’s use of wiping utilities was the subject of litigation to prevent exposure of damaging information. See, e.g., United States v. Gordon, 393 F.3d 1044 (9th Cir. 2004); Orrell v. Motorcarparts of Am., Inc., Civil No. 3:06CV418-R, 2007 WL 4287750 (W.D.N.C. Dec. 5, 2007); Commc’ns Ctr., Inc. v. Hewitt, No. Civ.S-03-1968 WBS KJ, 2005 WL 3277983 (E.D. Cal. Apr. 5, 2005); DirecTV, Inc., v. Borow, No. 03 C 2581, 2005 WL 43261 (N.D. Ill. Jan. 6, 2005). These e-discovery cases evidence equal opportunity infringers of rules of civil procedure in that plaintiffs and defendants used wiping utilities to erase or otherwise obscure damaging evidence.
\textsuperscript{164.} See \textit{Orrell}, 2007 WL 4287750, at *1; see also \textit{LANGE & NIMSGER, supra} note 126, at 222-24 (providing a line of cases demonstrating harm to a party’s case after that party attempts to destroy ESI).
data. In *Orrell v. Motocarparts of America, Inc.*,\(^{165}\) the plaintiff who wiped the hard drive had to produce the home computer for the defendant’s forensic expert to examine.\(^{166}\) In *DirecTV v. Borow*,\(^{167}\) the defendant who performed the wiping visited the website of an entity that pirated the plaintiff’s files via satellite.\(^{168}\) The plaintiff’s expert recovered some of the deleted programs.\(^{169}\)

A director of a corporation sued for breach of fiduciary duties may be tempted to use similar wiping utilities but may indeed suffer the same adverse consequence including sanctions, an adverse inference against the nonproducing party, or even dismissal of the entire case if the director is a plaintiff.\(^{170}\)

### F. Correlating Forensic Analytics with Fiduciary Duty Claims

Use of these forensic tools to gather and analyze information about corporate directors is obvious and ominous for a corporate director. Unwittingly, the seasoned director has thousands, if not millions, of communications over the course of his professional relationship with the corporation. The form of communication may range from mere e-mails and documents on his individual computer hard drive to Tweets, images and media on internal online programs, Facebook, or Linked-In, telephone conversations or messages retained on the company servers, and searches and data originating outside the company that are nonetheless retained on the company server or backup files. Even if the nefarious director successfully obliterated, buried, or otherwise lost his computer and hard drive, the corporation typically has backup tapes that systematically store the bulk of valuable information.

Assume a group of shareholders suspect a director has secretly profited from the sale of stock based on confidential information garnered through his corporate position. The director may indignantly assert the deletion of files was to simply retain only relevant information, therefore making it easier to search the files. Through metadata, however, forensic analytics could possibly ascertain the following information:

1. The date the director received confidential information;

---

169. *Id*.
170. See Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC, 685 F. Supp. 2d 456, 467 (S.D.N.Y. 2010) (suggesting that remedies are often asserted by the party seeking ESI).
(2) The dates certain e-mails were sent evidencing transmittal of confidential information originated from the director; and

(3) The date the target e-mails were deleted.

If the e-mails were deleted after the director’s receipt of the confidential information, and a chain of events showed the e-mails were sent to another company in which the director had a material financial interest, the shareholders have substantial proof against the director.

To date, there are no reported decisions where the court has relied primarily on electronically stored information (“ESI”) to hold a director liable for a breach of fiduciary duties. But as the rules, procedures, and forensic protocols evolve, ESI is likely to become important substantive evidence, which the parties may present to a jury or judicial fact-finder.

There are, however, breach of fiduciary duty actions that provide insight and foretell fiduciary challenges. In *Calyon v. Mizuho Securities USA Inc.,* plaintiff was a bank that alleged two of its senior executives “breached their fiduciary duties of undivided loyalty, good faith and fidelity” by actively participating in an illicit scheme that directly competed against the bank’s best interests. Specifically, the bank alleged the executives committed the following acts of breach:

1. Covertly inducing other bank employees to resign from the bank and join the defendant competitor;
2. Misappropriating confidential and proprietary business information to benefit the defendant;
3. Exploiting and diverting certain business opportunities to the defendant for their own personal benefit; and
4. Impairing the bank’s reputation and standing, prospective profits, and opportunities for profits.

The bank’s specific factual allegations gave rise to inevitable e-discovery issues. The complaint alleged that the executives induced other employees to terminate employment with the bank “in a coordinated fashion, without notice, and at a time and in a manner designed . . . to injure [plaintiff] . . . and to provide the maximum competitive benefit to defendants.” A savvy plaintiff’s counsel is likely to request e-mails and all other ESI that reveal all communications with plaintiff’s competitor. The claim of a “coordinated” scheme

---

174. *Id.* at *21.
will cause the plaintiff to retain a forensic investigator to examine date stamps of various e-mails and other ESI to show how those communications coordinated with other facts and events. The forensic examiner may look for digital anomalies, which if found may bring expert testimony that the executives had irregular behavior consistent with the atypical activity of sending employees to a competitor.

Plaintiffs would also likely use forensic investigation to buttress claims that the defendants intentionally used confidential information for the competitor's benefit and the defendants' personal gain. As discussed hypothetically above, any confidential or proprietary e-mails, documents, or electronically stored messages may have been deleted through overwriting programs and wiping methods. A forensic examination would search for deletion times, recovery of deleted data, and identification of the wiping or overwriting utilities and tools. If the plaintiff can establish that other directors have used the same brand of wiping tools, the plaintiff's position is enhanced.

The seriousness of such claims for executives and directors cannot be overstated. In Calyon, the bank requested compensatory damages of $150 million, punitive damages of $600 million, and various forms of injunctive relief to prevent further communication of proprietary information or solicitations damaging to the bank's reputation or profitability. Given the stakes, each party is likely to spare no expense in scouring all documents, including ESI, and securing quality forensic investigators to sift the ESI into a favorable web of events.

Not surprisingly, the e-discovery battles in Calyon were mostly resolved by stipulation, with the court issuing an order on the remaining issues. Importantly, the executives were required to do the following:

1. Produce their own forensic expert to consult with the bank's expert and coordinate a search of the “mirror images” of the executives' ESI, based on a protocol stipulated by the parties;
2. Preserve mirror images of all “computer hard drives and other storage devices in question”; and
3. If the bank established that any relevant mirror images were missing or had been withheld, or any other failure of the exec-

175. Id. at *31-32.
177. Calyon, 2007 WL 1468889, at *6. The term “Mirror Images” is a technical term essentially meaning a bit-by-bit copy of a computer hard drive designed to assure no alteration of an operating system during a forensic examination. Lange & Nimsger, supra note 126, at 408.
utives' forensic expert to consult with the bank's forensic expert existed, then the bank could renew its request for direct access to the mirror images of the executives' hard drives and other computer storage devices.\footnote{Id. at *6. Plaintiff's motion was to allow its own forensic expert to examine defendant's mirror images of hard drives and other computer storage devices, but the court denied that motion and instead only allowed plaintiff's expert to consult with defendant's expert, leaving direct access reserved to defendant's expert as long as defendant otherwise complied with the order. Id. at *1.}

Future counsel for corporate directors facing breach of fiduciary duty claims should anticipate similar production and discovery exposure. A director is likely to have used a computer for e-mail or other ESI. Any stored information that plaintiffs may perceive as disloyal or self-interested is likely discoverable and retrievable through a forensic examination. If the court is careful to control discovery, the protocol for mirror images may produce reliable exact, byte-by-byte duplicates of the originals. Admissibility of such potentially damaging evidence is then right around the corner.

G. Forensic Behavioral Analytics

Up to this point, this Article has discussed forensic analytics that have already gained a level of acceptance in the litigation context. The use of forensic experts to assist counsel in discovery of electronically stored information ("ESI") has existed for decades, as have sophisticated methods of retrieving deleted data. Reconstructing the chain of events is a bit more provocative because it is more circumstantial in nature. It attempts to make findings about a person's behavior without direct evidence of that behavior. That form of analytics nonetheless still analyzes a past behavior.

What appears more provocative is the use of recovered information to predict future behavior. The next logical question is how does this type of behavioral analytics apply to a breach of fiduciary duty claim against a corporate director? A director's past and current decisions have future consequences that may form the basis for a current breach of fiduciary duty.

Surely the business judgment rule, which prevents the court from interfering with good faith business decisions, is quickly claimed in a director's defense, but is not necessarily dispositive. As noted above, the various Model Business Corporation Act ("MBCA") defenses do not necessarily protect a director from an unreasonable judgment or unreasonable reliance on others' opinions. Some of those judgments and opinions may concern future actions. For example, a director may vote to authorize a distribution that is clearly beyond what the articles or
bylaws authorized. The director may have voted improperly on several past occasions. The director may then have engaged in several behaviors, say excessive consumption of alcohol or other actions that impaired his judgment on each of the prior occasions. Apart from prior acts that led to unauthorized distributions, could not those same acts (i.e. judgment impairing activities) support a fiduciary duty claim before the vote to provide unauthorized distributions? In other words, could forensic analytics uncover those judgment-impairing activities and predict the behavior on the eve of another distribution vote? If the plaintiffs sought injunctive relief, seeking to prevent the director from voting, would a court consider forensic evidence?

These are unanswered questions. While the director should only be required to be “reasonable” in making decisions, if a forensic investigation reveals that the director’s past and current actions make her unfit to make future decisions, injunctive relief would appear a possibility. Could that be a basis for a current breach of a fiduciary duty? To date, no case law has addressed the issue.

As noted above, the circumstantial aspect of forensic behavioral analytics, be it chain of events reconstruction or predictive analysis, is most provocative in that findings are made without actual facts to support those findings. The means of making those findings has to do with software development. Software development firms are continually developing ways of using computers to mimic or advance human decision-making. Indeed, one professor wrote an article over thirty years ago suggesting judicial decision-making could be supplanted by computer decision-making (machine intelligence) in some circumstances. Some scholars theorize that if many “things” can be converted to functional equivalent numbers, then a numbers-based computer is as functional, if not more so, than the human brain.

If the legal community accepts that premise, computer data may be a plausible means of re-creating facts and characterizing human

---

180. Injunctions are a form of equitable relief, most prominently requiring that irreparable harm would occur without the injunction, that there is no existing available remedy at law, and that the proponent is likely to prevail on the merits.

181. Computerized mimicking of human behavior is now an innovative part of the music industry. Yamaha Corporation developed software that created a Japanese pop star singing artist, Hatsune Miku, which is totally computer-generated, is performing in sold out concerts to crazed youth in Japan, and debuted in Los Angeles during the writing of this article. See Corey Takahashi, Digital Pop Star Hatsune Miku’s First Live US Concert, PRI’s THE WORLD (July 4, 2011), http://www.theworld.org/201107/digital-pop-star-hatsune-mikus-first-live-concert/.


decisions. While there may never be an end to the philosophical debate comparing human intelligence to artificial intelligence ("AI"), there is little question that in this digital age, AI has gained increasing acceptance in the law.\textsuperscript{184} The focus of the law is primarily on ESI. The rules of evidence and civil procedure have accommodated yet still struggle to clarify the use of ESI. Some cases have already allowed various forms of ESI in litigation as substantive evidence. Accordingly, the use of forensic examinations based on software designed to analyze or even mimic decisions of computer users is imminent.

The acceptance of AI leads to the possibility that ESI contains enough information for software programs to make findings regarding a corporate director's decisions and behavior. Shareholders are likely to request ESI evidencing the director's decisions as a basis for asserting a breach of fiduciary duty. The process of using data to predict behaviors is keyed to finding ever more qualitative ways of matching relationships among types of data. One software solutions firm has touted its semantic search technology that has "an unlimited number of dimensions of how words or charts are related to each other."\textsuperscript{185} Similarly, software used to analyze human behavior is based on electronically gathered information. One data mining application is used to detect fraud through an examination of prior acts for patterns of behavior.\textsuperscript{186}

In the case of health care fraud, data has been examined for repetitive patterns of billing irregularities and analysis of relationships among 200 million electronic claims records.\textsuperscript{187} The unusual behaviors are identified through such tools as statistical models and mathematical algorithms, allowing an entire population of data to be

\textsuperscript{184} The debate includes a threshold issue of what is unique about human intelligence. Arguably, the elements of human intelligence are four-fold: (1) consciousness, (2) a sense of self, (3) perception, and (4) language. Smith, supra note 183, at 277, 280. Others contend emotion and intuitive knowledge are necessary for action, and thus for intelligence, which machines do not replicate. See id. at 284, 286 (describing the tensions between deductive calculations and intuitive abilities). This Article focuses on corporate director decisions that are ostensibly designed for the best economic interests of the corporation but may involve a director's self-interest. Such decisions are rooted more in logic and economic interests than emotions and intuition. Thus, it could be said that there is contextual support for discussing the potential use of AI, that is, software programs' forensic investigations of ESI, for decision-making of corporate directors.


\textsuperscript{186} Colin Caffrey, Can a Computer Read a Doctor's Mind? Whether Using Data Mining as Proof in Healthcare Fraud Cases is Consistent with the Law of Evidence, 30 N. ILL. U. L. REV. 509, 509-10 (2010) (explaining the application to detect health care fraud).

\textsuperscript{187} Id. at 510.
analyzed.188 There have been several successful prosecutions involving medical fraud and smuggling of goods, both of which require plaintiffs to prove intent to commit the illegal act.189

A corporate director could also face allegations of fraud. The data to be mined may be a pool smaller than the millions of electronically billed medical records. Instead, primary sources of ESI may be emails, documents, and telephone calls about specific transactions. Unlike in gross negligence or breach of good faith suits, the plaintiff in a breach of fiduciary duty action does not need to prove the element of criminal intent.190 If criminal fraud cases, which are more challenging in document scope and evidentiary proof, have allowed successful prosecutions, then data-mined evidence of illegal behavior is quite plausible against corporate directors in a breach of fiduciary duty action. A corporate director’s breach of fiduciary duties may also stem from illegal acts, such as violations of the Foreign Corrupt Practices Act,191 backdating options to enhance value and price for the director, or acts that evidence misleading, inaccurate, or fraudulent reporting of financial statements.192

Perhaps just as much an omen, albeit outside of existing litigation, is the use of predictive behavior analytics to characterize the type of judgment used by corporate directors when voting by proxy. A recent project evaluated whether voting data can be used to predict value judgments of the directors, specifically whether the directors were more favorable to firm-generated proposals than minority shareholder proposals. In the proxy project, a “voting analytics” database compiled voting records for all 3,540 funds across “top 104 fund families.”193 The database included voting data for all mutual fund investors with a certain type of information, which was then refined by software programmers to a dataset sampling of 8,929 proposal-firm observations.194 One finding was that “mutual fund managers tend to vote more in favor of management than shareholder-sponsored pro-

188. See id. at 510-11.
189. See United States v. Erikson, 75 F.3d 470, 482 (9th Cir. 1996) (providing a discussion of a medical fraud case); see also United States v. Wales, 977 F.2d 1323, 1328 (9th Cir. 1992) (providing a discussion of a smuggling case); Caffrey, supra note 186.
190. See MODEL BUS. CORP. ACT § 8.30(a) (2005) (providing standards of conduct for board members).
193. Ng et al., supra note 74, at 4.
194. Id. at 10.
posals."  The analytics program also found that mutual fund companies were least supportive of what they termed "social and political" proposals. Those findings were used to corroborate the theory that "social and political proposals do not pertain to the economic mission of the corporation." The conclusion from those findings was that “mutual funds do not demonstrate a strongly [socially] responsible voting.”

If it is possible to use predictive behavioral analytics to find corroborative findings about proxy voting judgments, it may be equally possible to establish findings that show value judgments or predispositions in directors' voting. Minority shareholders may propose, for example, an environmentally responsible initiative that the directors and majority shareholders oppose because it erodes profits. If the minority shareholders believe the directors voted unfairly or with biases against the shareholders' or corporation's interests, they could bring a fiduciary claim. This type of predictive analytics to show directors' biases is easily imagined as part of the discovery process. If employers initiate such a study for internal purposes, the board may be in the unenviable position of having to produce such findings in response to a plaintiff's request for production of documents in a breach of fiduciary duty or fraud action.

H. Securities Claims

A potential companion of fiduciary duty claims against directors is securities violations claims. As with a fiduciary duty claim, shareholders can allege the directors or the corporation violated statutory duties to fully disclose information material to a potential investor's ability to make an informed decision. Such claims are related to fiduciary claims in that a securities violation (i.e. not fully advising potential and existing shareholders of negative information about the company, and therefore its stock) is similar to a director's failure to disclose to the shareholders that information misled them or was fraud. A securities violation also exists when a director profits from the sale of company stock outside of required reporting disclosures. That same occurrence is also grounds for a breach of a duty of loyalty and usurping a corporate opportunity. Hence, both securities fraud claims and breach of fiduciary duty claims are but multiple counts in the same complaint.

195. Id. at 11.
196. Id. at 13.
197. Id.
198. Id. at 20.
In Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities, LLC, ninety-six investors sued to recover losses of $550 million from two hedge funds in which they owned shares. They claimed the losses occurred from entity liquidations. The investors brought suit under federal and state securities laws against the former directors, administrators, auditor, and prime broker and custodian of the funds. The litigation focused on e-discovery issues, with the court holding that the investors failed to meet their discovery obligations to timely impose a litigation hold and preserve relevant documents. The investors formed an ad hoc committee to investigate the issues prior to filing suit. Presumably, the investors were well aware of cases like Gutman v. Klein, in which the court entered a default judgment against the defendants for what a court-appointed forensic expert determined were incidences of computer tampering by the defendant to permanently delete files and conceal the chronology of those deletions. Shareholders may easily envision similar motivations, tactics, and claims against corporate directors for fiduciary breaches, which can include the same factual basis for securities fraud. Indeed, electronic documents of a key executive have been discoverable in a securities fraud cases.

I. THE DANGER OF ADVERSE INFERENCES

The possibility exists that recovered e-mails give rise to inferences adverse to a director. Though the inference is not predictive of future behavior, it may be damaging. If a fact-finder is allowed to infer from a director’s failure to produce e-mails regarding his correspondence with a competing company that the director had conflicts of interest or secretly profited from his relationship with the competing company, that inference will obviously adversely affect the director’s defense.

A director’s sale of stock may also give rise to adverse inferences based on electronically stored information (“ESI”). As noted in the above chart, the corporate sale of stock is clearly within the realm of

204. Id.
205. See id. at 463 (providing sanctions for the plaintiffs’ negligence).
206. Id. at 472.
fiduciary duty claims where shareholders allege impropriety by a key executive in the transaction. In *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co.*,210 an e-discovery dispute arose when Coleman (Parent) Holdings, Inc. ("CPH") sued Morgan Stanley for fraud in connection with CPH's sale of stock in its subsidiary, Coleman, Inc.211 CPH was to receive stock of an unrelated company, Sunbeam. CPH alleged that Morgan Stanley had knowledge of a fraudulent scheme by Sunbeam.212

Central to CPH's case was the need to show Morgan Stanley's knowledge of the illicit scheme.213 CPH, therefore, aggressively sought discovery of Morgan Stanley's ESI. Morgan Stanley produced approximately 1,300 pages of e-mails.214 An outside vendor analyzed thousands of backup tapes. After Morgan Stanley's repeated failures to fully produce e-mails and backup tapes, noncompliance with the court's discovery orders, and apparent destruction of ESI, the court granted CPH's request for an adverse inference against Morgan Stanley as a non-producing defendant.215

The adverse inference is just another potential pitfall awaiting a director facing claims of fiduciary error. In *Coleman*, the court order carefully stated the scope of the inference.216 Specifically, the order stated that the court would provide the jury "conclusive" findings of fact.217 No inferences were to be drawn from those facts, but "counsel may make such argument to the jury in favor of whatever inferences that evidence may support."218 The evidence would likely include the results from CPH's forensic expert. As noted above, deliberate attempts to destroy documents can be detected or recovered. If the documentary evidence (i.e. forensic results) concludes that the deleted e-documents were sensitive strategy messages from or about Sunbeam, the permitted inference may be that forensic evidence revealed knowledge of the scheme. It is a parallel evidentiary matter to examine if a director had "knowledge" of confidential or proprietary company information. Such evidence could be damaging if there was a claim that the director breached his fiduciary duty by using that information to secretly profit at the corporation's expense.

213. *Id.*
214. *Id.*
215. *Id.* at *4-6, *7.
216. *Id.* at *1.
217. *Id.* at *7.
218. *Id.*
In Coleman, the court order further allowed CPH to argue that any concealment by Morgan Stanley "[was] evidence of its malice or evil intent," and Morgan Stanley had the burden of "proving to the jury . . . that it lacked knowledge of the Sunbeam fraud . . . ." A defendant director facing claims of fiduciary duty violations could face similar consequences if the defendant did not produce ESI containing damaging information to the plaintiffs.

Another adverse inference case is J.P. Morgan Chase Bank v. Liberty Mutual Life Insurance Co., in which J.P. Morgan Chase Bank ("Chase"), a holder of rights to receive oil and natural gas, sued Liberty Mutual Life Insurance Co. ("Liberty") to recover on surety bonds allegedly guaranteed by Liberty following Enron's insolvency. The court admitted e-mails from certain senior officials of Chase, but additionally determined that jurors could use those e-mails as probative evidence of Liberty's claim that the transactions in question were not insurable. While this use of recovered e-mails may bring favorable inferences to the defendant company, it is just as possible that recovered e-mails may damage the defendant's case. A court may issue jury instructions that allow an adverse inference against a defendant. In J.P. Morgan, the e-mails were used to suggest behavior (that the guarantees were made) not directly shown by the evidence. The defendant could be a corporate director, and plaintiffs may likewise use recovered e-mails to establish that the director made guarantees of corporate actions, and that it would be both a breach of contract and a breach of fiduciary duty to renege on that promise.

J. Maximum Director Protections

To present the most challenging aspect of this issue, assume that a company chooses to incorporate in a state that maximizes the liability shield available to its board of directors and executives. The state of choice is Delaware, which allows an organization to extinguish nearly all fiduciary duties through its governing documents. Section 102(b)(7) of the Delaware Code permits "eliminating or limiting" a director's personal liability for monetary damages for a breach of a fiduciary duty. There are a few notable exceptions. Section 102(b)(7) further states the liability shield does not exist "[f]or any breach of the director's duty[,] . . . for acts or omissions not in good faith or which

---

219. Id.
222. JPMorgan, 2002 WL 31867731, at *1 (explaining how the lack of insurability resulted from the transactions being classified as "off-the-books").
involve intentional misconduct or a knowing violation of law[, or] . . . for any transaction from which the director derived an improper personal benefit.” Requirements of good faith and avoidance of adverse improper personal benefit are still present in the hypothetical situations this Article addresses. Like in the scenarios based on the Model Business Corporation Act (“MBCA”) above, corporate directors should be wary of the potential use of forensic evidence under the Delaware Code.

This Article also suggests the director's fiduciary duty must be expanded to include an awareness of modern theories when overseeing assets. In *Brane v. Roth*,224 the court held that directors of a grain cooperative breached their fiduciary duties by retaining a manager inexperienced in “hedging,” the cutting-edge practice of reducing the risk to company assets through the use of derivative securities.225 According to the court, the breach also included the failure of the directors to “maintain reasonable supervision over [the inexperienced hedge fund manager], and failing to attain knowledge of the basic fundamentals of hedging . . . .”226 The corporation gained ninety percent of its income from long grain transactions, and the director's failure to employ accepted hedging techniques damaged the company.227 Most relevant to this Article is the court's decision that the practice of hedging was a legitimate business expectation.228

The reasonable business expectation of shareholders should, in my view, increase as forensic science gains acceptance and use within enlightened corporations. The above discussion of the state of the science in this area is ample evidence that anyone with responsibility to oversee operations can use e-mail-sifting algorithms to flag irregular behaviors. Behaviors that should be discovered at an early stage could prevent actual damages or wasting of corporate assets. The failure, therefore, of directors to meet the *Brane* fiduciary standard of knowledge and supervision could result in a breach of fiduciary claim against the uninformed directors.

The fiduciary duty could even be expanded to include predictive behavior tools discussed above. The theory is that directors have put in place a risk manager with access to forensics that evidence digital anomalies within electronically stored information (“ESI”). Arguably, directors that do not know the basics, or know only enough to supervise those with the forensic responsibility, have breached their duties.

227. *Id.*
228. *See id.* at 591 (explaining that grain elevators should hedge to protect corporate earnings).
The material harm is that adequate use of those tools would have discovered the grave errors before they happened.

A similar expansion of the fiduciary duty standard to meet contemporary innovations has also been introduced to property trustees. While the trustees' fiduciary standard is a "prudent investor rule," the fundamental tenants are aligned with the corporate director fiduciary standard. Directors of corporations, like trustees of a beneficiary's property, are stewards of the assets belonging to others, be it a corporation or an individual. The prudent investor standard, as with corporate fiduciary duty rules, includes a requirement of reasonable knowledge by the trustee. Academic literature, however, also suggests the need for a trustee to have "working" knowledge of modern theories on how to manage a beneficiary's portfolio. According to the rule that a director view his duty based on a prudent person "in similar circumstances," a director should be able to consider technological advances of forensic tools that discover financial reporting errors within a CRM system or other tools of investigation of e-mail irregularities, such as DEDICOM.

K. Financial Reporting Enhancements

A director's responsibility should incorporate oversight of financial reporting to assure shareholders and the potential investing public that the earnings are accurately reported. One corrective technology in response to the corporate scandals involving Enron, WorldCom, Tyco, Qwest, and HealthSouth, is the increased identification of a practice termed cosmetic earnings management ("CEM"). One example of CEM is artificially placing unmanipulated income below a certain key user reference just above the threshold. For example, $499 million in earnings is changed to reflect $501 million in

230. The "prudent investor rule" requires a trustee to be reasonably knowledgeable or have professional advice on behalf of a beneficiary. See id. at 138 n.53.
231. See id.
232. See id. at 141.
233. The director’s oversight functions are repeatedly and broadly stated in the Model Business Corporation Act. See Model Bus. Corp. Act § 8.30(b)-(c) (2005). Those provisions should be read to be harmonious with subsection (e) of that section, which entitles a director to rely on the opinions, reports, and financial statements and other financial data prepared by others. See Model Bus. Corp. Act § 8.30(e). Subsection (e) of that section clarifies that reliance is not allowed if the director knows that reliance is unwarranted. Id. By necessary implication, therefore, the judgment required to determine whether reliance is warranted is part of the oversight function of a director.
earnings. While the difference in the actual amount of earnings could be viewed as relatively minor, the sole purpose of the technique is "deception with the intent of swaying user judgment." Even minor increases in income can bring significant increases in company value based on market perceptions.

Methods have been developed to detect such fraudulent manipulation of financial data. The various cosmetic manipulations of financial data have been sufficiently exposed to be within a director's constructive knowledge or oversight. Since CEM involves management of earnings, the failure to incorporate state of the art management techniques to control potential deception in financial reporting lies at the liability doorstep of directors. The increased technological methods of finding CEM abuses are therefore also the immediate responsibility of those directors. The impact of such technology is actually two-fold: a director with nefarious designs has a greater chance of being discovered, and even if there is no bad faith, the reasonable oversight burden increases given the advent of modern technologies.

L. The Impact of Social Media

A director, bluntly stated, could be a victim—an old dog being tricked by new technology. For example, a director may have learned how to use an application ("App") on his iPhone. But significant bits of information can be learned from his use of that App, unbeknownst to him. Such data mining is also part of forensic data recovery and analysis. The same can be said for social media, where a director is lured into Facebook for family purposes and then other workers, friends, and associates connected tangentially with his work are slowly infused into the fold. Perhaps a director's once latent excesses or judgmental improprieties find an avenue of expression through social media. The information is potentially recoverable, discoverable, and subject to chain of events re-creations and other predictions of a director's behavior.

235. Id. at 37. Another example is where a depreciable asset's useful life is extended, thus increasing the income that can be reported. See id. at 33.
236. See id.
237. See id. (testing for the presence of CEM allows managers to find ways to boost income).
238. Smartphone applications have been the source of privacy concerns by consumers and even federal authorities, but prosecutions are rare, and smartphone manufacturers continue to routinely datamine information about their users and provide the information to third parties without disclosure to the phone user. See Amir Efrati et al., Mobile-App Makers Face U.S. Privacy Investigations, WALL STREET J., April 5, 2011, http://online.wsj.com/article/SB10001424052748703806304576242923804770968.html.
Media analysts have already concluded that the Internet changes the way people think and communicate. 239 One college dean succinctly stated, “The Internet has become an extension of my memory . . . It combats the occasional senior moment, helping me to find names, facts, and places nearly instantly. It gives me a second, bigger brain.” 240 A director of a major corporation may have to adapt to an increasingly complex, global, and evolving business environment. He may find the second, bigger brain quite alluring. Unwittingly, he may also find searches he performed to “investigate” a competitor with whom he eventually invested may reappear in a breach of fiduciary duty case even though he deleted the search from his computer or used a wiping utility to eliminate it from the deleted files on his hard drive.241

V. CONCLUSION

This Article addressed the risks in shareholder lawsuits against directors for breaches of fiduciary duties. This Article outlined various emerging challenges not generally contemplated or litigated. As a species, humans may well be creatures of habit. If so, in this age of artificial intelligence and forensic analytics, the deviation from habit can be more readily flagged than ever before with digital anomalies and a host of software programs that create algorithms. The consequences, therefore, are likely to be more adverse for the deviant corporate director attempting to avoid breach of fiduciary duty claims. To remain reasonable in judgment and oversight, a scrupulous director may have an increased responsibility to be knowledgeable about modern technology and remain reasonable in judgment and oversight.

A greater concern for directors involving forensic experts is whether they are prepared for the arms race to convince a court of its own forensic protocol. To date, studies show a general unpreparedness for e-discovery in a majority of the corporations reviewed. This Article has presented numerous scenarios illustrating the potentially devastating consequences in personal liability to a director if the forensic arms race is lost.

239. See JOHN BROCKMAN, IS THE INTERNET CHANGING THE WAY YOU THINK: THE NET'S IMPACT ON OUR MINDS AND FUTURE (2011) (“The Internet is the infinite oscillation of our collective consciousness interacting with itself.”).
241. The more expansive impact of social networks on corporate directors and executives is the subject of a future article by this author, Corporate Directors Caught in the Web of the Internet and Social Media.