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

Roger M Groves, Florida Coastal School of Law
ABSTRACT: Millions of documents, including five million messages, termed electronically stored information (“ESI”) from the Enron litigation have provided an opportunity for software developers to create software that analyzes ESI for behaviors of computer users in more provocative and innovative ways than previously encountered. The law is struggling to clarify e-discovery rules, but the ambiguities provide an opportunity for counsel to manipulate or take advantage of forensic investigations. In this article, the author examines the potential exploitation of e-discovery forensic tools by shareholders of a corporation that suspect a breach of fiduciary duties by members of the board of directors.
TABLE OF CONTENTS

INTRODUCTION ......................................................................................................................... 1

PART ONE ................................................................................................................................... 2

ELECTRONICALLY STORED INFORMATION IN LITIGATION ............................................... 2

The Scope of the E-Discovery Problem and Underpinnings for Forensic Analytics ............. 3
Platforms ................................................................................................................................... 5
Enronic Embryonics of Forensic Analytics ............................................................................. 6
State of the Science ................................................................................................................... 7
Predictive Analytics .................................................................................................................. 10
Email Analytics ......................................................................................................................... 14
Contextual Forensic Evidence in Litigation ............................................................................. 14

PART TWO .................................................................................................................................. 16

ISSUES OF PROCEDURE AND ADMISSIBILITY ................................................................... 16

Litigation Hold and Search Protocol: ......................................................................................... 16
Forensic Opportunities and Consequences ................................................................................ 16

PART THREE ............................................................................................................................... 20

SUBSTANTIVE CLAIMS AGAINST DIRECTORS ................................................................. 20

FOR BREACH FIDUCIARY DUTY .............................................................................................. 20

Plaintiffs’ Quiver of Claims – A Wide Array of Theories and Causes of Action ............... 20
The Defendants ......................................................................................................................... 24
Defining the “Duty” in the Digital World ................................................................................ 25
Data Recovery and Analysis ..................................................................................................... 26
The Preeminent Importance of Metadata and Unveiling Attempts to Destroy Evidence .... 28
Correlating Forensic Analytics with Fiduciary Duty Claims ................................................ 31
Forensic Behavioral Analytics .................................................................................................. 33
Securities Claims ....................................................................................................................... 37
The Danger of Adverse Inferences ......................................................................................... 38
Even with Maximum Director Protections ................................................................................ 40
Financial Reporting Enhancements ......................................................................................... 42
The Impact of Social Media ....................................................................................................... 42
THE IMPLICATIONS OF A JEOPARDY! COMPUTER NAMED WATSON: BEATING CORPORATE BOARDS OF DIRECTORS AT FIDUCIARY DUTIES?

Roger M. Groves

“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.”¹

“Now artificial intelligence software has taken a seat at the negotiating table.”²

INTRODUCTION

Can my employer look at my emails, cell phone calls, instant messages, Facebook, and Twitter accounts over the past few 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 emails 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.³

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.⁴ The industry is forensic examination and sifting of ESI to discover trends and make findings as to who did what based on ESI regained by the company. The industry of forensic analytics found its oasis in


³ Analytics in this context refers to software products that construct “complex models of organizational behavior, allowing any deviations from normal behavior to be more easily identified.” See the website of Cataphora, a premier patent holder for one such software program used for investigations and litigation at http://www.cataphora.com/releases/release/cataphora-reveals-latest-advanced-social-network-data-analysis-technologies/ (last visited July 13, 2011). Synonymous terms are forensic analytics or social analytics. Visual Analytics is another term to refer to a reasoning process created by software that “maximizes the human capacity to perceive, understand and reason about complex and dynamic data and situations.” See The Science of Analytic Reasoning, Illuminating the Path. http://nvac.pnl.gov/docs/RD_Agenda_NVAC_chapter2.pdf (quote is printed, article in full is saved on hard drive as “Evidence Analytics Article – Analytics Definition”).

those Enron documents, now known as the “Enron Corpus”. Pretrial discovery is now thrust onto a technological landscape that 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.

The e-discovery ambiguities and uncertainties provide an opportunity for counsel to manipulate or take advantage of forensic investigations as part of the e-discovery. In this article, the author examines the potential exploitation of e-discovery forensic tools by shareholders of a corporation that suspect a breach of fiduciary duties by members of the board of directors. Accordingly, this article is organized to highlight the background and evolution of e-discovery in Part One. This is followed by more a more detailed discussion of specific types of forensic evidence as applied to litigation and potentially fiduciary duty claims. Part Three applies the various forms forensic analytics to breach of fiduciary duty claims by shareholders.

PART ONE
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 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 were amended to specifically provide guidance to attorneys concerning their duties in requesting and responding to discovery. Not surprisingly, the rules could not cure all the potential ambiguities and crafty

---


8 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)(5). 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)(6). And more notably, the court must receive a report from the attorneys as part of their 26(f) conference that includes those e-discovery items. Fed R. Civ. P. 26(f). Rule 26(f) specifically now states that the conferences include: “any issues relating to disclosure or discovery of electronically stored information...Fed. R. Civ. P. 26(f)(3).
attempts to prevail by respective counsel, so there are numerous federal court decisions that attempt to add additional clarity to e-discovery issues.⁹ Some cases provide sanctions for discovery improprieties, other do not. Some select or threaten from an array of other remedies for e-discovery violations.¹⁰

**The Scope of the E-Discovery Problem and Underpinnings for Forensic Analytics.**

The advisory committee tasked with amending the Federal Rules of Civil Procedure to address e-discovery issues identified four major reasons why amendments were necessary.¹¹ 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 was that the sheer volume of ESI dwarfs any traditional concept of scope known in the primarily paper record era. According to Committee findings, “…ninety-five percent of all information is now generated in digital form, [and] all document discovery is or will soon be e-discovery.”¹² A major corporation may easily have 10,000 tapes of information.¹³ Just one tape is the equivalent of a “200-mile high stack of paper”¹⁴.

The second impetus for e-discovery rules is the “dynamic nature” of ESI, since it continues to grow and evolve.¹⁵ Eerily similar to fictional horror films of man versus machines, computers automatically create and store information without human operator advice or knowledge.¹⁶

---

⁹ Among the most recent and comprehensive attempts to provide the blueprint for e-discovery rules is most notably The Pension Committee of the University of Montreal Pension Plan, et al., v. Banc of America Securities, LLC, et al. 685 F. Supp. 2d 456 (2010).


¹¹ See 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. See Shira A. Scheindlin, E-Discovery article, p 1. Judge Scheindlin was a member of that Committee.


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 includes the creator of the information, when last accessed, last edited.\(^\text{17}\)

Saliently for this paper, metadata also includes “clues to human behavior.”\(^\text{18}\) 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…”\(^\text{19}\)

The utility of this metadata, particularly its potential to “exonerate and incriminate”, is brought to fruition through the forensic analytics discussed in this article. And 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 rules is simply because unlike paper records, electronic records are practically impossible to delete.\(^\text{20}\) A corporate employee that hits the delete key only moves the data to a more remote location.\(^\text{21}\) Though more expensive or time consuming, the data is not only recoverable but discoverable.\(^\text{22}\) 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 than existing in with paper records.\(^\text{23}\) In an age of accelerated technological advances, it is entirely possible that ESI was initially stored in devices that are now obsolete, or was part of an inaccessible or poorly organized prior format.\(^\text{24}\)


Translating information to current formats may be costly and time consuming. These retrieval burdens add to the burden of being a director defendant, obligated to produce ESI from obsolete storage devices.

For defendant directors, the retrieval and translation problem may be compounded by the possibility of multiple plaintiffs. Shareholders are contemplated in this article as plaintiffs, but the director’s fiduciary duties run to both the shareholders and the corporation. Therefore the corporation could conceivably be another plaintiff along with shareholders, but 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 the director’s misdeeds. An individual director could easily be overmatched in that arm’s race for forensic experts. The consequences of losing the forensic war can be grave, as discussed below.

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, the forensic analytics is not confined to the mere retrieval of electronic documents in “as is” condition. Forensic experts can also generate additional findings from that data – findings that may identify behavior patterns of the computer user. Those patterns are therefore documentary sources for fiduciary duty liability not otherwise contemplated by corporate officers, employees or directors.

Platforms

In addition to the above unique challenges of ESI compared to paper record production in discovery, there is a challenge due to 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. Electronically stored information may also be contained in “personal digital assistants (PDA’s), laptops, thumb drives, telephone calls placed through the internet (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 plaintiff investigation will have his or her communications analyzed from an unprecedented array of comprehensive sources. Directors with questionable

---

26 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. See MBCA § 8.63(a).
27 There is just as conceivably 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 the indemnification does not cover certain acts that could bring a breach of fiduciary claim – e.g. a director’s individual fraud or embezzlement or other felony.
activities may avoid excoriating communications on the lap top but still have damaging information revealed from an alternate source. Plaintiffs’ forensic investigators and counsel likewise have numerous opportunities for corroboration and increased reliability of forensic findings.

**Enron Embryonics of Forensic Analytics.**

Forensic analysis in litigation owes much of its development to the corporate scandals from early in this millennium. In the fall of 2001, Ken Lay, the 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 to themselves more than $100 million in bonuses. A host of criminal prosecutions followed against the CEO, former President and CEO Jeff Skilling and Chief Accounting Officer Richard Causey. Prior to, during and after those criminal prosecutions, personal liability for a breach of fiduciary duties was looming against those same Enron executives.

In light of impending liability, some corporations have had a paper-shredding party in anticipation or in conjunction with their pity party. Not completely so with Enron. As described by one technology observer, “…as 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 conducted an investigation of Enron. That investigation led to the discovery of 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 for 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 other research projects and tests, including Carnegie Mellon University. Carnegie used the database to explore how humans, as opposed to machines, decide to organize data and classify messages. This was accomplished in large part by analyzing user threads and folders. Other researchers used the Enron Corpus to develop the “Enron Email Visualization and Clustering Tool” designed to create “graph-based visualizations

---

30 There were so many prosecutions, one scholar devoted an entire law review article to tracking the trials of the forty-six defendants and respective verdicts and guilty pleas. See Kathleen F. Brickley, *In Enron’s Wake: Corporate Executives on Trial*, 96 J. Crim L. & Criminology 397 (2005-2006).
33 The researcher was Mr. Andrew McCallum at the University of Massachusetts. See Michael Castelluccio, *The Enron Corpus*, STRATEGIC FINANCE, Vol. 92, Issue 11, p. 67, May 2011.
34 This Corpus includes 619,446 messages from 159 difference users. See Michael Castelluccio, *The Enron Corpus*, STRATEGIC FINANCE, Vol. 92, Issue 11, p. 67, May 2011.
of social networks within Enron, based on e-mail interactions between users.” Another group of researchers used the Corpus to test “Link Discovery” techniques, which were used to “ferret out fraud and terrorist activities” based on the ESI of the company.

Corporate directors are charged with statutory oversight functions in the many states that follow the MBCA. 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 plaintiff claim of a breach of fiduciary duties. The visualization of social networks developed by forensic experts 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 Corpus-tested methodologies were just the beginning. As more dramatically stated, the testing of data from the Enron Corpus “has become an unending academic autopsy courtesy of one of the most spectacular corporate deaths in modern times.”

State of the Science

As will be discussed below, forensic evidence based on artificial intelligence and related software programs cannot have relevance to potential fiduciary duty litigation unless there is a real threat and opportunity for expert witness testimony and acceptance of their theories and documentary evidence. Accordingly 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 then is what is the scientific foundation for the forensic evidence and how did it evolve specifically in the litigation context beyond Enron 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 that to “scour files and corporate e-mails for evidence and insights into company behavior”, and (2) assist law firms who conduct forensic examination of a

37 This research was conducted at the University of California, at Berkeley. See Michael Castelluccio, The Enron Corpus, STRATEGIC FINANCE, Vol. 92, Issue 11, p. 68, May 2011.
38 This research was conducted at the University of Southern California. See Michael Castelluccio, The Enron Corpus, STRATEGIC FINANCE, Vol. 92, Issue 11, p. 68, May 2011.
39 The scope of fiduciary duties is governed primarily by state law. See Robert W. Hamilton, Jonathan R. Macey, and Douglas K. Moll, Cases and Materials on Corporations, Including Partnerships and Limited Liability Companies, 11th ed. West, 2010, p. 653. The MBCA includes a provision that directors have a duty of due diligence, i.e. to become “informed in connection with their decision-making function” and the duty of reasonable oversight MBCA § 8.30(b).
40 Shareholders can file an action to remove a director “engaged in fraudulent conduct with respect to the corporation or its shareholders...” MBCA § 8.09(a). Obviously fraud is inconsistent with a director’s obligation to act in good faith and within the best interests of the corporation under Section 8.30. MBCA § 8.30(a).
business client’s files in anticipation of litigation. 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.”

Another company, Cataphora, has developed software that has been described as being able to “detect and comment on sentiment” based on an analysis of electronic messages. The software looks for “digital anomalies” by recognizing changes in vocabulary or tone within the communications. A compelling assertion by the founder of Cataphora to the New York Times includes 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.”

Additional revelations about the Cataphora programs and that of and 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’.” Cataphora uses this tool to be able to detect a person’s activities and interactions to ascertain “ who did what when, and who talks to whom...[so as to] visualize chains of events”, be it e-mail, instant messages, telephone calls or other electronic media.

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

---

48 Cataphora’s founder is Elizabeth Charnock. See New York Times Article
“…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.”

Specific tools have been developed for the recognition of 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.”

Subtle changes in the style of an e-mail message from casual to atypically formal are also detected and can “raise a red flag about illegal activity.”

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.”

Counsel for shareholders claiming a director breached fiduciary duties would likely retain at forensic firm with Cataphora capabilities to examine each and every email, 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 directors’ every word would be scrutinized. A computer would seem to be the only “person” able to sift 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-discovery 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, a Silicon Valley firm developed a visual presentation of general concepts based on electronic documents. The law firm that retained the firm for litigation purposes was able to analyze and sort search a half-million documents within the one-week period imposed by the court. In one day, over 3,000 “relevant”

---


documents were identified, in total allowing one attorney to “do work that might have once required hundreds.”

If therefore 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 ESI to be analyzed. Competent plaintiffs’ counsel will likely be aware of the forensic possibilities. If significant economic damages are at stake, the director(s) should expect plaintiff to use these sophisticated tools. It appears to leave the defendants with little choice but to anti-up, engage in the forensic arms war or face defeat, if no other reason, from the inability to refute the computer-generated findings of plaintiff’s forensic experts at a reasonable expense and on a timely basis during discovery.

A defense counsel may attempt to foreclose such provocative forensic evidence as not being part of a reliable industry or science. To refute such claims, plaintiffs can site firms like Cataphora that claims to have Fortune 500 companies, 100 law firms and federal agencies. Thus, any courts inclined to believe that any findings or analysis that requires judgment is reserved for humans must face a growing body of work to the contrary. Identifying and measuring a person’s “sentiment” is certainly commonly regarded a judgment call. The impressive client list of Cataphora seems to indicate highly sophisticated entities and agencies have already placed enough credence in this artificial evidence to pay to create it.

**Predictive Analytics**

The use of artificial intelligence to predict human behavior is also a developing part of forensic analytics. Within banking and telecommunications, there is a dramatic increase in demand for algorithms and computer models, sometimes with hundreds of the two operating simultaneously. These complex systems have been used to ascertain when a customer is 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 or PA” to establish a protocol for interventions in hopes of retaining the disaffected customer.59

Consider the potential use of PA in legal controversies. A company may use PA to target employees for termination. That may lead to a wrongful termination suit against that employer. If, conversely, the plaintiff retained a software programmer that had a PA tool that claims the employee was performing tasks consistent with company practice and procedure, the admissibility of such evidence could go to the heart of the substantive issue in plaintiff’s wrongful termination suit. And to the point of this article, it is conceivable that a PA tool could bring findings that a member of the board of directors, or a committee member appointed by the directors, had accessed competitor websites, 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 interests of the corporation. The PA tool could also be used to graphically show trigger dates that show a pattern of behavior adverse to the company.

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 in isolation may be excused as a reasonable use of business judgment.60 But if several opportunities to purchase the competitor are ignored coupled with other knowledge, like a familial relationship with the competitor are revealed, then at some point along the chronology of ignored opportunities, there is a more likely breach of the fiduciary duty to the company. The ability then to correlate call logs, wireless browsing histories, and communications with those family members who prevented exercising the business opportunity can be major factual points for plaintiff shareholders against the directors.

PA tools have already been successfully used in other business circumstances. One PA tool analyzed various demographics of current customers to help decide when the customer could not afford a particular plan, and when the company should offer a lesser plan.61 The PA tool was attributed to customer retention worth nearly $40 million annually.62 Harrah’s Entertainment is a gambling conglomerate of more than 40 casinos that has been using PA tools for over five years.63 Harrah’s system tracks 10 million customers and vast amounts of customer transactions

59 These predictive analytics are discussed in the context of customer retention management or “CRM”. Eric Narkin, CRM and Predictive Analytics, CRM Magazine, Vol. 15, Issue 5, p. 20, 21 May 2011. A Protocol has been defined as rules that govern the “communication and the transfer of data between machines, as in a computer system.” Webster’s New World College Dictionary, Fourth ed., Wiley Publications, Inc., 2010.
60 The business judgment rule is the subject of voluminous legal literature among courts and academes. See a list of law review articles, Robert W. Hamilton, Jonathan R. Macey, and Douglas K. Moll, Cases and Materials on Corporations, Including Partnerships and Limited Liability Companies, 11th ed. West, 2010, p. 653. Similarly, Section 8.31 (a) of the MBCA provides its version in a safe harbor from personal liability when a director is acting in a manner reasonably appropriate under the circumstances. MBCA § 8.31(a)(2)(ii)(B). In this author’s view, as facts change so should the reasonable expectations.
within Harrah’s resorts. These current behaviors are then used to either make additional offers of Harrah services as part of its Total Rewards program or cease marketing to those individuals.64 One Harrah executive bluntly described the value of its PA tools: “Really it’s about understanding which customers are performing worse than others.”65

Quite conceivably, a company may also use such 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 she eats, shops, vacations, or gambles from ESI. The aggregate information could then be used by the corporation to decide whether a director is using judgments or behaviors that are antithetical to the best interests of the corporation. 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. And 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.

Predictive Analytics has also been used to define and target prospective customers from the vast social media networks.66 The sources of a computer user’s behavioral information are well established - social network profiles, posts, click histories and usage logs to name some of the most prominent.67 The PA tool can be used to “discover links among people, organizations, businesses that would otherwise escape…attention.”68 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.”69

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”).70 The Algos are increasingly used to measure public sentiment. One such Algo used information from Twitter and correlated it with the Dow

---

66 The commentator first notes that Facebook and Twitter has amassed an enormous user base far beyond opt-in business models. So mining data from those free and open social networks is fertile ground for more behavioral analytics. Eric Narkin, *CRM and Predictive Analytics*, CRM Magazine, Vol. 15, Issue 5, p. 20, 22 May 2011.
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.

The relevance of predictive analytics from social media or smart phone usage to this article is that companies can track social network usage of its directors. Directors of a corporation are likely to have smart phones that are provided by the corporation. The company can retrieve and then opine about whether a director’s activities indicate patterns of collusion adverse to the interests of the company. What’s 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 unilaterally when to click on certain website items, and when (after hours perhaps) he were to make clandestine calls or web-based searches. As noted above, Algos are already being developed that correlate wholly legitimate electronic searches of the stock market with other information to ascertain sentiments of the user. 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 has already arisen whether mutual fund proxy statements are predictive of responsible decision-making.

The company or a group of shareholders suspecting foul play by the director may potentially use such predictive analytics to track an unsuspecting director-user of social media. Obviously, a
director that Tweet’s self-identified naked photos, or click on websites involving human trafficking or child pornography is subject to potential personal liability. Less obvious, but still a potential source of director removal from the firm are behaviors antithetical to the culture of the company. 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.

**Email 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 emails. The model is termed DEDICOM. As forensic tools find irregularities within the exchange of emails among board members and outside competitors, or with third parties not in the interests of the company, exposure of those exchanges increases, as does the potential for breach of fiduciary claims against those directors using the firm’s email 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 emails can be data mined to discern employee’s interests. Such research was conducted to better ascertain individuals with clandestine interests with the potential to be insider threats to the military. 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.

**Contextual Forensic Evidence in Litigation**

The legal field has already begun grappling with how to incorporate forensic software programs during confabs among legal experts in federal civil procedure. The Duke Conference of the Federal Civil Rules Advisory Committee convened in May 2010 amid calls for uniform e-


discovery rules.\textsuperscript{77} The Committee noted that computer algorithms have increasing use for “clustering, predictive coding, initial document culling, and other search technologies.” \textsuperscript{78} Predictive coding is another label for the attempts of software to use electronic information to form judgments about human behavior. So that technique was contemplated if not directly encountered in civil litigation.

Other evidence of recognized forensic analytics is found within a study of litigated issues in e-discovery.\textsuperscript{79} From among the 84 most significant e-discovery cases during 2010, the study analyzed the frequency with which certain categories of e-discovery issues were addressed. In 17\% of the cases, procedural issues involving “search protocol” were addressed, and another 8\% dealt with broader computer forensics protocols and forensic experts.\textsuperscript{80}

Thus, among the cases that involved significant e-discovery issues, one of every four concerned whether the software program, with its algorithms, is 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. Several illustrations have already been provided in this article 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 will be discussed below, the more forensic examination is considered to be a “science” or “skill”, the greater the opportunity for admissibility of expert testimony and 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

\textsuperscript{77} Information Management, (15352897)[ no individual author], Vol. 45, Issue 2, p. 14, March-April 2011.

\textsuperscript{78} Information Management, (15352897)[ no individual author], Vol. 45, Issue 2, p. 14, March-April 2011. Italics added by this author.

\textsuperscript{79} The company Kroll Ontrack examined 84 of the most significant e-discovery cases of 2010. See pie-chart summary of results at Information Management, (15352897)[ no individual author], Vol. 45, Issue 2, p. 14, March-April 2011.

\textsuperscript{80} Information Management, (15352897)[ no individual author], Vol. 45, Issue 2, p. 14, March-April 2011.
reasoning skills and compete against humans has already occurred. It was a historic battle of a computer named Watson versus the intellectually gifted among our species.81

It does not take much imagination to envis Watson’s brain with Cataphora-like forensic software – software that is used to match wits with defense counsel. Imagine Watson claiming in monotone, “the emails of director X of this corporation show digital anomalies from June 2, 2006 through August 27, 2011, on 1149 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 that mimics and convicts the director. But as feared by one commentator, only Watson committed to memory the Enron Corpus and testing methodology to assure reliability of the findings. 82 A director and defense counsel without a Watson of their own is at serious risk of being defenseless.

PART TWO
ISSUES OF PROCEDURE AND ADMISSIBILITY

Litigation Hold and Search Protocol:
Forensic Opportunities and Consequences

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

Forensic evidence is part of ESI. The courts have considered ESI in litigation so often in the past few decades that e-discovery is its own sub-titled jurisprudence.83 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,

“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.” Fujitsu Ltd. v. Federal Express Corp., 247 F.3d 423, 436 (2d Cir.2001)

81 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.


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. Nor is there an excuse from this obligation if he or she had reasonable access to customary communication regarding such information.

This constructive knowledge leads to an affirmative obligation to preserve – i.e. place a “litigation hold” on potentially relevant documents, including ESI.84

Of particular relevance to this article is the next step. As was the case in Treppel, the parties may not agree on what ESI must be preserved. After motions to expand or narrow the scope of what is discoverable, the Court may enter an order clarifying three obligations on the party producing ESI:

1. That the defendant corporation conduct a search
2. That the search explain its “search protocol”
3. That the defendant produce responsive documents consistent with that search protocol.85

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 defendant with the sole risk of responsive production.86 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 circumstance. The search may reveal potentially incriminating evidence about the corporation’s own employees, officers and directors. And following the Treppel test, the failure to follow that protocol and produce documents therefrom could result in significant sanctions or other remedies.87 The defendant corporation is caught in the legally uncomfortable position of having to preserve the very evidence that can damage the defenses of its own elected directors.

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 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

84 In the Court’s words, “[o]nce 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, 220 F.R.D. 212, 218 (S.D.N.Y.2003) (“Zubulake IV”).
86 Understandably the plaintiff may have had a war mentality and refused to let defendant “off the hook” or make life easier.
87 Those remedies include significant monetary sanctions, adverse inferences in jury instructions against the nonproducing party, and even default judgments against that party. See Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 218 (S.D.N.Y.2003) (“Zubulake IV”) and Gutman, U.S. Dist. LEXIS 97707, 2008 WL 5084182. Thus the failure to comply is not a viable option.
with 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 46% of US companies and 41% of British companies have a policy addressing e-discovery readiness; facing instead these issues 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 future potential admissions, inferences, or disadvantages in proofs of a defendant. 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 market share, profitability and share value of the company. One particular director was most powerful, influential and the swing vote among the board members. The director purposefully and repeatedly voted against the purchase. A group of shareholders alleges that the director has close relatives on the board of the competitor and has not only a conflict of interest but self-dealing and personally profits more from the separation of companies than the purchase.

The plaintiff shareholders may only have thin unsubstantiated allegations at the commencement of litigation. But if their forensic expert establishes a protocol that required the director and the corporation to produce information showing the director’s communications with or about the competitor, to be organized and presented according to the plaintiff’s protocol, digital anomalies and links in communication that evidence clandestine insider threats pattern of communication between the defendant director and the relatives in the competing corporation could be almost assured if the forensic evidence is believed by a jury. That would in turn be prime evidence of self-dealing and conflicts of interest in breach of his fiduciary duties.

This author predicts therefore that this very early stage of discovery may increasingly become a more intense battleground than existing 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 it may also win the war.

---

88 The study was conducted by Kroll Ontrack, entitled “The 2009 ESI Trends Report”, reported at Information Management, (15352897) [no individual author], Vol. 44, Issue1, p. 20 (Jan-Feb 2010).
89 Management, (15352897) [no individual author], Vol. 44, Issue1, p. 20 (Jan-Feb 2010).
There are a host of additional evidentiary issues, many of which are already subject to substantial scholarly discussion.\(^90\) One primary issue involves whether a forensic programmer and analyst could qualify as an expert witness. FRE 702 governs the admissibility of testimony that is based on “scientific, technical, or other specialized knowledge.”\(^91\) Since we are dealing with cutting edge forensics, it is significant that the Advisory Committee’s Note explicitly recommended a broad interpretation of the types of knowledge experts can use in developing an opinion. In the Committee’s words,

The field 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.’\(^92\)

The Committee further rejects confining experts “in the strictest sense of the word” to traditional occupations as “physicians, physicists, and architects”.\(^93\) Specifically included via 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 as expert witnesses the forensic analysts with behavioral conclusions from mathematical algorithms. While they certainly could already be classified as have technical knowledge, they more certainly can be offered as having training and education in the skill of developing software designed to analyze the actions of users of ESI. The emerging field that draws behavioral conclusions appears comfortably within the “specialized” knowledge now allowed under FRE 702.\(^94\)

The obvious companion of forensic expert testimony is the written and technical report relied upon by expert. FRE 703 includes explicit allowance of facts or data that is “of a type reasonable relied upon by experts in the particular field.”\(^95\) 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. Arguable, since FRE 702 has a broad view of the “knowledge” requirement for expert testimony, (including those with non-traditional “skills”)


\(^{91}\) Fed. R. Evid. 702.

\(^{92}\) Advisory Committee’s Note to Rule 702 at 56 F.R.D. 183, 282.

\(^{93}\) Advisory Committee’s Note to Rule 702 at 56 F.R.D. 183, 282.

\(^{94}\) Advisory Committee’s Note to Rule 702 at 56 F.R.D. 183, 282.

\(^{95}\) No discussion of scientific expert testimony is complete, however, without including the landmark case of Daubert v. Merrell Dow Pharmaceuticals, Inc., and its progeny. Daubert v Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993). While Daubert appears to have a rather restrictive five-part test for admissibility, several courts and commentators oppose 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 Paul F. Rothstein, Federal Rules of Evidence, Thomson Reuters (2010), p. 908; Kumho Tire Co. v. Carmichael, 119 S. Ct. 1167, 1175 (1999) and Kannankeril v. Terminix Int’l. Inc., 128 F. 3d 802, 809 (1997).

\(^{95}\) Fed. R. Evid. 703.
the scope of a “particular field” under FRE 703 is likewise broadened. Stated differently, if forensic programmers of behavior analytics are part of group with “skill” or “specialized” knowledge sufficient to provide testimony as experts, it would be consistent to also broadly define the “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 algos and models. FRE 901(b)(9) is frequently used to authenticate computer-generated information.96 A process or system, as is forensic program, must meet two foundation requirements for admissibility. First, it must be described. Secondly is 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 sufficiently familiar with its operation. A body of law has already developed, though evolving, to authenticate computer-generated evidence, including digital animation, simulations, and computerized models.97 As noted by one commentator, computer-generated evidence has been used, “to construct hypothetical markets in an antitrust claim for purposes of illustrating anticompetitive behavior.”98 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 fiduciary duty obligations of directors.

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.

PART THREE
SUBSTANTIVE CLAIMS AGAINST DIRECTORS FOR BREACH FIDUCIARY DUTY

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

Directors of a corporation occupy a position of trust and confidence to act in the interests of the corporation they serve.99 As such they are fiduciaries with affirmative duties to act or avoid acting against those interests.100 Broadly stated, directors have a duty of care and a duty of loyalty.101 There is however a rather complex web of these duties, due in part to the

96 Fed. R. Evic. 901(b)(9).
100 The 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.” MBCA § 8.30(a).
101 The statutory duty of care is principally found in Section 8.30 of the MBCA. MBCA § 8.30. The duty of loyalty is principally lodged at MBCA § 8.60 and § 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.
interrelationship between case law and statutory provisions within various states. At times state legislatures’ react to statutory provision, and at times case law reacts to the statutory provision. Those dynamics give rise to some variance from state to state. Yet, a substantial majority of states follow relatively closely to the MBCA. The Delaware corporate statutes are also viewed as an influential guidepost so this article will examine principal provisions from both the MBCA and Delaware business statutory formulations, and some of the interpretive case law.

Another factor that adds to the complexity is judicial interpretations of good faith and the business judgment rule. 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 good faith is required for directors under the MBCA, but remains an undefined term. For the purposes of this article, this author prefers to view them as any defendant director may have to – as separate counts in a complaint since there is sufficient case law where courts have viewed the doctrines as being based in common law, sufficiently independent from a state’s business statute. Courts, for example, have linked a lack of good faith to defeating the corporation’s attempt to absolve itself of liability through the use the business judgment rule.

Two other factors add to the complex web of fiduciary duties for a director. First there are independent sources of liability within separate bodies of laws and subjects that could give rise to fiduciary duty claims. Secondly, 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 is a source apart from state statutes for a plaintiff’s claim. The list of some primary characterizations of fiduciary breaches is noted below, presumably any one of which a court may find sufficient if established to hold a director or the corporation liable.

102 Reportedly, three-fourths of the states engrafted the MBCA’s standard duty of care. See William E. Knepper and Dan A. Bailey, The Liability of Corporate Officers and Directors, Matthew Bender & Company, 2010, Eighth Ed., §3.02 at p. 3-3.
103 See BJR discussion, supra, note 60.
104 See list of articles regarding the business judgment rule, supra, at note 60 and definition at infra, note 119.
106 There are for example 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. There are also federal antifraud provisions and insider trading rules, and personal liability for directors under federal environmental laws.
107 Under the MBCA, a director could have a separate basis for personal liability for self-dealing - conflict of interest transactions (MBCA § 8.60), than when voting for unauthorized distributions to shareholders (MBCA § 8.33), or acting in bad faith or not reasonably in the best interests of the corporation. (MBCA § 8.30).
108 Securities statutes in federal and state law, if violated, could obviously bring potential companion claims that could be investigated through forensic tools, but are beyond the scope of this article.
109 See the statutory references within the chart and generally, William E. Knepper and Dan A. Bailey, The Liability of Corporate Officers and Directors, Matthew Bender & Company, 2010, eighth ed., p. 2-1 through 4-56.
<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 - MBCA § 8.30(a)</td>
</tr>
<tr>
<td>Failure to discharge duties using reasonable belief in best</td>
<td>Duty of Care - MBCA § 8.30(b)</td>
</tr>
<tr>
<td>interests of the corporation</td>
<td></td>
</tr>
<tr>
<td>Inadequate disclosure of material information needed for decision-</td>
<td>Duty of Care - MBCA § 8.30(c)</td>
</tr>
<tr>
<td>making or oversight functions</td>
<td></td>
</tr>
<tr>
<td>Reliance on information knowing such reliance is unwarranted</td>
<td>Duty of Care - MBCA § 8.30(d)</td>
</tr>
<tr>
<td>Delegating to and reliance on others who the director cannot</td>
<td>Duty of Care - MBCA § 8.30(d)(f)</td>
</tr>
<tr>
<td>reasonably believe have the “skills or expertise” to be reliable and</td>
<td></td>
</tr>
<tr>
<td>competent</td>
<td></td>
</tr>
<tr>
<td>Reliance on information, opinions or reports of others who the</td>
<td>Duty of Care - MBCA § 8.30(e)(f)</td>
</tr>
<tr>
<td>director cannot reasonably believe is reliable and competent</td>
<td></td>
</tr>
<tr>
<td>Conflict of interest in transactions when the director or a related</td>
<td>Duty of Loyalty - MBCA § 8. 60</td>
</tr>
<tr>
<td>person had material financial interest that was unfair to the</td>
<td></td>
</tr>
<tr>
<td>corporation without disclosing the existence and nature of the</td>
<td></td>
</tr>
<tr>
<td>conflict and without ratification by disinterested directors of the</td>
<td></td>
</tr>
<tr>
<td>corporation</td>
<td></td>
</tr>
<tr>
<td>Failure to act in good faith (i.e. acting with a purpose other than</td>
<td>Duty of Loyalty – Case Law.¹¹⁰</td>
</tr>
<tr>
<td>for the best interests of the corporation)</td>
<td></td>
</tr>
<tr>
<td>Acting arbitrarily or for laudable purposes instead of the best</td>
<td>Duty of Loyalty – Case Law¹¹¹</td>
</tr>
<tr>
<td>interests of the corporation.</td>
<td></td>
</tr>
<tr>
<td>Appropriating a “Corporate Opportunity”</td>
<td>Duty of Loyalty – Case Law¹¹²</td>
</tr>
<tr>
<td>Failure to fully disclose “material” facts from the view of a</td>
<td>Duty of Fair Dealing – Case Law¹¹³</td>
</tr>
<tr>
<td>reasonable shareholder.</td>
<td></td>
</tr>
</tbody>
</table>

¹¹⁰ See In re Walt Disney Company Derivative Litigation, 906 A. 2d 27, at 67-68 (2008); Stone v Ritter, 911 A. 2d 362 (2006), and the line of cases noted at William E. Knepper and Dan A. Bailey, The Liability of Corporate Officers and Directors, Matthew Bender & Company, 2010, eighth ed., note 10 at p. 4-4. It is worth noting that the duty of loyalty is not confined to just conflict of interest transactions. See Stone v Ritter, 911 A. 2d 362. And while that case 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. See discussion at William E. Knepper and Dan A. Bailey, The Liability of Corporate Officers and Directors, Matthew Bender & Company, 2010, eighth ed. at p. 4-3. Other cases broadly state the same fundamental requirement of refraining to act in a way that subrogates the interests of the corporation to his own personal interests though the bad faith label was not attached. In re Allegheny Int’l, Inc. 954 F. 2d 167, 180 (1992).


¹¹² 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 the corporate assets. In re Safety International, Inc., 775 F. 2d 660, 662 (1985).

¹¹³ See Loudon v. Archer-Daniels-Midland Co., 700 A. 2d 135, 143 (1997). See also the line of cases supporting the duty of disclosure at William E. Knepper and Dan A. Bailey, The Liability of Corporate Officers and Directors, Matthew Bender & Company, 2010, eighth ed., p. 4-8 through 4-10.1. The duty of fair dealing is generally attributed The American law Institute, and is regarded as very similar to the conflict of interest prohibitions, both of which involve the selfinterested director in a transaction affecting the corporation. See William E. Knepper and Dan A. Bailey, The Liability of Corporate Officers and Directors, Matthew Bender & Company, 2010, eighth ed., Section 4.03, p. 4-7.
Trading shares based on confidential information acquired through the director’s fiduciary position  
Taking unfair advantage of corporate procedures, program, or operations to maintain control against the interests of the corporation and its shareholders.  
In selling controlling shares, (1) Freezing out minority or less favored shareholders or directors in corporate transactions; or (2) failing to make an offer to sell controlling interests equally available to other shareholders; or (3) failing to sell shares that is inherently fair to the corporation  
Selling shares and transferring control to those who may “loot” the corporation.

These claims are not available in all jurisdictions, but nonetheless provide a range of potential plaintiff challenges to a director’s actions within the general claim of a breach of fiduciary duties. 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 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. Those cases are examined because one of the most likely sources for director liability is the company’s own shareholders who claim that a director’s failures can be revealed from the recovery of voluminous ESI from the director that caused an adverse consequence to the corporation.

---

115 Bennett v. Breuil Petroleum Corp., 99 A. 2d 236 (1953). The key element being the improper purpose that is against the interests of the entity; a director’s desire to maintain control through the purchase shares or solicitation of proxies is not itself improper or a breach of fiduciary duty. Rosenfeld v. Fairchild Engine & Airplane Corp., 130 N.E. 2d 610 (1955).
116 The equal opportunity test was articulated in a California case, Jones v. J. F. Ahmanson & Co., 460 P. 2d 464 (1969), but as not gained traction judicially or statutorily. See discussion at William E. Knepper and Dan A. Bailey, The Liability of Corporate Officers and Directors, Matthew Bender & Company, 2010, eighth ed., § 4.08, p 4-20. The inherent fairness test incorporates the notion of fair dealing where the duty of loyalty is violated if there is a failure to adequately disclose material facts of self-interest, and that if the transaction occurs it will generate a significant financial benefit to the self-interested director. Jones v. H. F. Ahmanson & Co., 460 P. 2d 464 (1969).
117 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. Col, 727 F. 2d 1480 (1984) and cited cases therein. If a director is a majority shareholder, that duty runs from her to the corporation and also minority shareholders. Harris v. Carter, 582 A. 2d 222 (1990).
118 The other apparent source may be a former employee who files a wrongful termination suit against not only the corporation, but also its directors.
There are several defenses available to directors. But this article examines the risks of liability in light of forensic ESI analysis 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, and reasonable as a person in a like position, or relying on opinions of others that she reasonably believes to be reliable and competent. Thus, the director risks are still very high if a plaintiff uses ESI to establish unreasonable actions or acts of omission by a director.

The Defendants

Directors of a corporation are generally required, but do not have to be a shareholder unless prescribed by the articles of incorporation or bylaws. And there is no general statutory prohibition against a director also being an officer or other executive within the corporation. So a director 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 qualifications of the position.

---

119 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, MBCA § 8.62, or if the transactions falls outside of the detailed definition of a “Director’s conflicting interest transaction” MBCA § 8.60 and MBCA § 8.61 (a), or there is ratification by a majority of the shareholders to transaction that qualifies as a conflicting interest transaction under the statute. MBCA § 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 as long as there is to abuse of discretion, fraud or illegality. See International Ins. Co. v Johns, 874 F. 2d 1447, 1461 (1989); Auerback v Bennett, 393 N.E. 2d 994 (1979); In re Oracle Corp. Derivative Litigation, 808 A 2d. 1206 (2002). 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 action is not in the best interests of the corporation. MBCA § 7.44. There are several other motions defense counsel can assert to prevent production of documents or testimony, including but not limited to attorney-client privilege, undue burden, lack of reliability and hearsay, and violations of the Electronic Communications Privacy Act. See where such defense claims were successful in In re Subpoena Duces Tecum to AOL, LLC, 2008 WL 1956266 9 E.D. Va. April 18, 2008, and related discussion at Michele C.S. Lange and Kristin M. Nimsger, Electronic Evidence and Discovery: What Every Lawyer Should Know Now, American Bar Association, 2nd ed, (2009), p. 274.

120 For reasonableness as a director requirement to act in good faith and in the best interests of the corporation see MBCA § 8.30(a); for like person reasonableness in oversight functions, see MBCA § 8. 30(b), and for reasonable reliance on the opinions or reports of others see MBCA § 8.30(f).

121 See MBCA § 8.01 (a) and MBCA § 8.02.

122 See MBCA § 8.02 which allows the articles or bylaws to proscribe qualifications for directors.
The Enron prosecutions provide a broad scope of potential executives potentially subject to civil liability for breach of fiduciary duties.\textsuperscript{123} Twelve of the forty-six defendants that went to trial held the title of Chief Executive Officer, Chief Operating Officer, President, Chairman of the Board and Senior Partner of related partnerships. Also included as defendants were the Executive or Senior Vice President, Investment Advisor, Chief Legal Officer, and Vice President for Legal Affairs.\textsuperscript{124} There are also committees established by the board of directors, with directors able to statutorily able to serve on a committee, unless the articles of bylaws state otherwise.\textsuperscript{125} So any of those persons holding any of those positions could have also been directors and subject to breach of fiduciary duty claims by shareholders.

**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.\textsuperscript{126} A primary potential source of conflict between corporate director fiduciaries and the corporation and its shareholders can be explained in terms of a director’s pressure to fulfill multiple, sometimes conflicting obligations. Directors are stewards for the corporate best interests, and those interests are often about increasing financial performance and value for the corporation and its shareholders.\textsuperscript{127} Factors affecting that performance include the pressure to produce ever-increasing profits and assets, while lowering debt service.\textsuperscript{128} In the case of Enron, the core legal issues involved a pattern of accounting and audit failures and misdeeds.\textsuperscript{129} Self-interested transactions, cover ups, and document obfuscation occurred, originating from a common temptation to increase profitability, albeit beyond the bounds of the law. 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. Unless we believe executives at Enron 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 cases for breaches of fiduciary duties against those with the same title as the executives in Enron and other corporations rocked with the scandals early this century.

\textsuperscript{123} The Enron litigation primarily involved criminal fraud but the alleged egregious actions would provide the factual basis for similar civil claims.
\textsuperscript{125} See MBCA § 8.25(a).
\textsuperscript{126} See MBCA § 8.31(a) which references liability to “the corporation or its shareholders” and MBCA § 8.63(a) which concerns an action by shareholders for a director’s conflict of interest transaction.
\textsuperscript{129} The well-documented improprieties include the abuse of certain “related-party” partnerships to show phenomenal success. See Perry E. Wallace, *Accounting, Auditing, and Audit Committees After Enron*, 43 Washburn L. J. 91, 100 (2003-2004).
The shareholder-plaintiff’s quiver of claims above is generically sourced from historical development of cases and statutes in business law jurisprudence. The advent of 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 that accommodate the ESI complexity and burden.\textsuperscript{130} To the thesis of this article, those same reasons present a need to analyze the impact of ESI, not just for litigation generally but on the actions specifically against directors and their fiduciary duties.

The potential for forensic evidence to assist plaintiffs is apparent. The left column of the claims list presents 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 categories in various ways that would not have been contemplated in a pre-digital world. Put more ominously, consider the various means now available for software programmers can use forensic tools to access years of emails, cell phone calls, documents stored on hard drives, or remote storage devices, which are beyond the mental capacity of the director to recall. So while the sources and definitions of the fiduciary duty have not been altered by the digital age, the recovery of information that may establish those violations has – and therein lies the potential for more aggressive plaintiff actions and the need for heightened awareness of all communications by corporate directors.

**Data Recovery and Analysis**

Plaintiff’s counsel typically utilize a three-step forensic process, commencing with retention of a forensic expert that develops a strategy to collect and analyze data, followed by the actual data recovery and analysis, and then expert report and testimony.\textsuperscript{131} This article focuses on the data recovery and analysis, because the director’s risks are ascertained therefrom.

There are numerous avenues available to a forensic examiner to retrieve a director’s ESI. It is important to note that forensic tools can collect data from virtually any storage device, even antiquated or damaged systems.\textsuperscript{132} So a director has no safe harbor in obsolete computer systems discarded by the corporation.

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.\textsuperscript{133} Importantly, the image also reveals any unused areas and user “overwriting” where old data is

\textsuperscript{130} See the above discussion supra at note 5, where the sheer volume of emails, inter alia, and evolved means of sifting data and analyzing behaviors required special rule amendments.


\textsuperscript{133} A byte is a collection of “bits” that computers use to represent a character, e.g. “a” or “1”. 1 million bytes is a megabyte, and 1 billion bytes is a gigabyte. Michele C.S. Lange, Kristen M. Nimsger, *Electronic Evidence and Discovery: What Every Lawyer Should Know Now*, American Bar Association, 2009, p. 210-11. p. 401.
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 emails.

Particularly relevant to this article is the next 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 software scanning of 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;
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 allegations of breach of fiduciary duties. Many of the factual scenarios giving rise to claims of breach as noted in the above chart involve affirmative acts of the director. Misappropriation of a corporate opportunity is one of many such acts, and plaintiffs’ ideal proofs would show a nexus first between the director and the opportunity, and secondly that the opportunity was only available through the 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 computer used by the director was owned by the corporation, that drafts of

135 There may also be on-site data collection. This process involves imaging at the company’s location, the company’s main servers and individual director and employee computers. There are various methods to verify the accuracy of the images compared to the original data (“hashing” through computer algorithms) and assure that the process used in creating the copy maintained authenticity of the data, e.g. chain of custody logs. See Michele C.S. Lange, Kristen M. Nimsger, *Electronic Evidence and Discovery: What Every Lawyer Should Know Now*, American Bar Association, 2009, p. 213-14.
damaging documents were originally authored by the director and deleted only after the notice of plaintiffs’ action.

A successful plaintiff then would establish that the corporation could have reasonably desired involvement in the opportunity and the requisite resources. An analysis of traditional patterns of emails 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 all evidence a chain of events and patterns of conduct that plaintiffs could pursue to the potential detriment of a defendant director.

The Preeminent Importance of Metadata and Unveiling Attempts to Destroy Evidence

The ability to discover and analyze computer information often depends on metadata. It has been described as “data about data – the who, what, where, why, and how about a file.”138 Software programs, file systems, and operating systems create and store metadata (e.g. when a file was created, last modified, size of file, etc.).139 Each program or system has unique features within its own metadata that enhances the ability to locate and isolate sources of information.140 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.”141

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.142 The storage device within the computer has files, some used, others unused. Every new booting up of the computer can modify the metadata of the files in the new and used space, and even temporary cache files. Thus even the start up by a director user gives “clues” to the history of computer usage.143 This is a process that is part of what is termed “overwriting” of existing files.

Metadata is now established as part of discovery in litigation, including civil claims as with a fiduciary duty allegation. Courts have explicitly rejected defendant’s argument that metadata is inherently not part of the documents and therefore is not to be produced in discovery.144

139 Michele C.S. Lange, Kristen M. Nimsger, Electronic Evidence and Discovery: What Every Lawyer Should Know Now, American Bar Association, 2009, p. 233. Operating systems are the software that other software depends on to make a computer functional. Lange, Electronic Evidence, p. 232.
141 See metadata discussion above, supra, pg 28.
prominent case for this point involves a defendant corporation that resisted production of electronic spreadsheets (Microsoft Excel). The defendant explained that it scrubbed the metadata from the spreadsheets so plaintiffs could not “undelete” or otherwise recover privileged information from the spreadsheets. The court admitted 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.”

But the Court emphasized that “metadata is the key to showing the relationships between data” and without metadata, certain data would have minimal meaning. Accordingly, the Court 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 making the changes, and elimination on final versus draft versions of spreadsheets appear relevant and must be disclosed.

Posit the circumstance then where a corporate director has compromising information on spreadsheets that shareholders claim reveals his efforts to freeze out shareholders, or secretly profit from transactions, or 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, the analysis can reveal far more about surrounding facts than the document facts themselves. All such information can buttress such claims about a director’s knowledge or intent to scheme at the expense of the corporation.

Another method of data destruction is known as “wiping”. The effort is to clean the computer data for a subsequent use, as an IT department may prepare a computer for sale to a third party or redeployed within the company. Some forensic experts have made observations that could implicate the director fiduciary issue directly.

“…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.”

146 Williams v. Sprint/United Management Col, 2320 F.R.D. 640 (D. Kan. 2005). The court also noted that most metadata is not visible when a document is printed, but can be altered intentionally or unintentionally.
What may not be known to the nefarious user is that forensics experts can often still identify the “date, time, and specific program used to conduct the wiping.” Coupled with other facts, a circumstantial case may still be plausibly made against the computer user – in our case - a corporate director.

In *Kucala Enters, Ltd. v. Auto Wax Co.* a forensic expert determined that the night prior to imaging of original files, a wiping utility was used to delete and overwrite over 12,000 files, and that 3,000 more files were deleted and overwritten three days earlier. The expert identified the brand name of the wiping utility, and claimed that the same product has been used in several other cases where either the plaintiff or defendant destroyed computer evidence in the face of litigation. There is now a line of cases exposing a party’s attempt to destroy ESI that is harmful to that party’s case.

This wiping utility line of cases also reveals the creative efforts of an opposing party, authorized by the court, to find alternate means of gathering data. In *Orrell v. Motocarparts of Am. Incl.*, a plaintiff that wiped the hard drive had to produce the home computer for the defendant’s forensic expert to examine. In *DirecTV v. Borow*, the defendant that performed the wiping visited the website of an entity that pirated plaintiff’s files via satellite. Plaintiff’s expert recovered some of those deleted programs.

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 – sanctions, an adverse inference against the nonproducing party in the substantive case, and even potential dismissal of the entire case if the director was a plaintiff.

---


153 The wiping utility is boldly labeled “Evidence Eliminator”. Other products are more innocuously labeled – Window Washer, Cyberscrub to name a few. Other cases where a party’s use of wiping utilities was the subject of litigation to prevent exposure of damaging information include *Orrell v Motorcarparts of Am., Inc.*, 2007 WL 4287750 (W.D.N.C. Dec. 5, 2007); *Commc’ns Ctr., Inc. v. Hewitt*, 2005 WL 3277983 (E.D. Cal. Apr. 5, 2005); *DirecTV, Inc., v. Borow*, 2005 WL 43261 (N.D. Ill. Jan. 6, 2005); *United States v. Gordon*, 393 F. 3d 1044 (2004). These e-discovery cases evidence equal opportunity infringers of rules of civil procedure. Plaintiffs and defendants used wiping utility to erase or otherwise obscure damaging evidence.

154 See *Orrell v Motorcarparts of Am., Inc.*, 2007 WL 4287750 (W.D.N.C. Dec. 5, 2007) and the line of cases noted in *Electronic Evidence and Discovery*, p. 222-224.


157 Those remedies are now often asserted by the party seeking ESI. See *The Pension Committee of the University of Montreal Pension Plan, et al., v. Banc of America Securities, LLC. et al.* 685 F. Supp. 2d 456 (2010).
Correlating Forensic Analytics with Fiduciary Duty Claims

The application 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 a professional relationship with a corporation. The form of communication may range from mere emails, 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 back up files. Even if the nefarious one successfully obliterated, buried, or otherwise lost the computer itself 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 and therefore make it easier to search files. Through metadata, however, the following information could possibly ascertained through forensic analytics:

1. The date the director received confidential information
2. The dates certain emails were sent evidencing transmittal of confidential information originated from the director.
3. The date the target emails were deleted.

If the emails were deleted after the director’s receipt of the confidential information, and a chain of events is established showing that the emails were sent to another company in which he had material financial interest, the shareholders have substantial proofs against that director.

There are no reported decisions located to date where the substantive claims of fiduciary duty breach have been decided against a director based primarily on ESI. But as the rules procedures and forensic protocols become more settled, more claims are likely to become substantive evidence and presented to a jury or judicial fact finder.

However, there have been existing plaintiff actions for breach of fiduciary duty that provide insight and foretell fiduciary challenges. In *Calyon v. Mizuho Securities USA Inc., et al*, plaintiff is a bank alleging that two of its senior executives breached their fiduciary duties “of undivided loyalty, good faith and fidelity” by actively participated in an illicit scheme of a direct competitor against the best interests of the plaintiff. Specifically, plaintiff alleges the executives committed the following acts of breach:

---

1. Covertly inducing other plaintiff bank employees to resign from plaintiff bank and join the defendant competitor;
2. Misappropriating confidential and proprietary business information to benefit defendant;
3. Exploiting and diverting certain business opportunities to defendant for their own personal benefit; and
4. Impairing plaintiffs’ reputation and standing, prospective profits and opportunities for profits.159

Plaintiff’s specific factual allegations give rise to inevitable e-discovery issues. The complaint alleges, for example, that the executives induced other employees to terminate employment with the plaintiff “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 [themselves].

A savvy plaintiff’s counsel is likely to request emails and all other ESI that reveals all communications with plaintiff’s competitor. The claim of a ‘coordinated” scheme will cause the plaintiff to retain a forensic investigator to examine date stamps of various emails and other ESI to show the coordination of those communications with other facts and events. The forensic examiner may look for the digital anomalies, which if found may bring expert testimony that the executives had irregular behavior that is consistent with the atypical activity of sending employees to a competitor.

Plaintiffs would also likely use forensic investigation to buttress claims that confidential information was intentionally used for the competitor and the personal gain of the executives. As discussed hypothetically above, if the executives sent emails, documents, or any electronically stored messages to the competitor that could be deemed confidential or proprietary, those communications may have been deleted through overwriting programs and wiping methods. The forensic examination would search for timing of deletes, recovery of deleted data, and identification of the wiping or overwriting utilities and tools. And if the brand name of the wiping tools can be correlated to other improper uses by other corporate directors as part of case precedent, the plaintiff’s position in enhanced.

The seriousness of such claims cannot be understated for these senior executives or any directors of a corporation. In Calyon, the plaintiff requests 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 that damage the plaintiff reputation or profitability. Accordingly, each party is likely to spare no expense in scouring all documents, including ESI, and paying whatever is necessary to secure qualitative forensic investigators to sift the ESI into a favorable web of events.

159 The plaintiff also alleged a less-emphasized count of Computer Fraud and Abuse Act violations. Complaint, p. 19.
Not surprisingly, e-discovery battles ensued in Calyon, but were resolved mostly by stipulation and a court order was issued on remaining issues.\textsuperscript{160} Importantly, the defendants were required to do the following:

1. Produce their own forensic expert for consultation with plaintiff’s expert to coordinate a search of the “mirror images” of defendants ESI, based on a protocol stipulated between the parties;\textsuperscript{161}
2. Preserve mirror images of all computer hard drives and other storage devices in question;
3. If plaintiff establishes that any relevant mirror images are missing or have been withheld, or other failure of defendant’s forensic expert to consult with plaintiff’s forensic expert, then plaintiff may renew its request for direct access to the mirror images of defendant’s hard drives and other computer storage devices.\textsuperscript{162}

Future counsel for corporate directors facing breach of fiduciary duty claims should anticipate similar production and discovery exposure. The director is likely to have used a computer for email 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 with controlling the discovery, the protocol for mirror images may produce reliable byte-by-byte exact duplicates between the mirror images and the original. Admissibility of such potentially damaging evidence is then right around the corner.

**Forensic Behavioral Analytics**

The discussion to this point has involved forensic analytics that has already gained a level of acceptance in the litigation context. The use of forensic experts to assist counsel in ESI discovery has existed for decades, as have sophisticated methods of retrieving deleted data. The chain of events reconstruction discussed above 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. This section goes beyond this point of analysis.

What appears more provocative is the use of recovered information to predict a future behavior. The next logical question is how can that type of behavioral analytics apply to a breach of fiduciary duty claim against a corporate director? Arguably, a director’s fiduciary duties can be

\textsuperscript{160}See the Court Order at 2007 WL 1468889 (S.D.N.Y. May 19, 2007).
\textsuperscript{161}The term “Mirror Images” is a technical term essential meaning a bit-by-bit copy of a computer hard drive designed to assure no alteration of an operating system during a forensic examination. Michele C.S. Lange and Kristin M. Nimsger, *Electronic Evidence and Discovery: What Every Lawyer Should Know Now*, American Bar Association, 2\textsuperscript{nd} ed, (2009), p. 408.
\textsuperscript{162}Plaintiff’s motion was to allow its own forensic expert to examine defendant’s mirror images of hard drives and other computer storage devices. 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.
pasts, current and futuristic. That is to say, it is plausible that past and current decisions made by directors involve the future in that egregious failures today regarding the future could be a basis for a current breach of fiduciary duty.

Surely the business judgment rule – banning the court from interfering with good faith business decisions - is quickly interposed in a director’s defense, but is not necessarily dispositive. As noted above, the various MBCA defenses do not necessarily protect a director from an unreasonable judgment or unreasonable reliance on the opinions of others. And some of those judgments and opinions may concern future actions. For example, a director may vote to authorize a distribution that clearly is beyond what is authorized under the articles or bylaws. 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 impair his judgment on each of the prior occasions. Apart from the potential breaches from prior acts that actually led to unauthorized distributions, could not those same precursor actions (judgment impairing activities) alone be a basis of fiduciary duty claims even 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 plaintiffs sought injunctive relief, seeking to prevent the director from voting, would a court consider forensic evidence, assuming other factors do not cause a dismissal of the case?

These are unanswered questions. And while certainly the director should only be held to being “reasonable” at the current time of making decisions, if forensic investigation reveals that the past and current actions of the director make her unfit to make future decisions, injunctive relief would appear a possibility.163 Could that be a basis for a current breach of a fiduciary duty? No case law has been located to addresses that 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 the actual facts to support those findings. The means of making those findings has to do with software development. Software development firms are continually evolving ways of using computers to mimic or advance human decision making.164 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.165 And a body of scholars theorizes that if many “things” can be converted to functional equivalent numbers, then

---

163 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.

164 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) that is totally computer generated, and is performing in sold out concerts to crazed youth in Japan, and debuted in Los Angeles during the writing of this article. See PRI The World radio program transcript at [http://www.theworld.org/2011/07/digital-pop-star-hatsune-mikus-first-live-concert/](http://www.theworld.org/2011/07/digital-pop-star-hatsune-mikus-first-live-concert/) (last visited July 4, 2011).

decision making from a numbers-based computer is as functional, or more so than the human brain.  

If the legal community accepts that premise, computer–derived data may likewise be a plausible means of re-creating facts and characterizing human decisions. While there may never be an end to the philosophical debate about the similarity or difference between human intelligence and artificial intelligence (“AI”), there is little questioning that in this digital age, AI has gained increasing acceptance in the law. The language of the law among litigants and practitioners is primarily stored electronically (“ESI”). The rules of evidence and civil procedure have accommodated and still struggle to clarify the use of ESI. Some cases have already allowed various forms of ESI in litigation as substantive evidence. So 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 as to a corporate director’s decisions and other behavior. Shareholders are likely to request the ESI relative to those decisions as a basis for asserting breaches of the director’s fiduciary duty.

This process of using data to be predictive of behaviors is keyed to finding ever more qualitative ways of matching relationships among types of data. One software solutions firm touts its semantic search technology that has “an unlimited number of dimensions of how words or charts are related to each other.” Similarly, software is used to analyze human behavior based on electronically gathered information. One data mining application is to detect fraud through an examination of prior acts for patterns of behavior.

---


167 The debate includes a threshold issue of what is unique about human intelligence. Arguable the elements of human intelligence are four fold: (1) consciousness, (2) a sense of self (3) perception and (4) language. See J.C. Smith, *Machine Intelligence and Legal Reasoning*, 73 Chi-Kent L. Rev. 277, 280. Others contend emotion and intuitive knowledge are necessary for action, and thus for intelligence, which machines do not replicate. Smith, p. 284 and p. 286. This article focuses on corporate director decisions ostensibly at least designed for the economic best interests of the corporation, that may instead involve his own self-interest. Such decisions are rooted more in logic and economic interests, than emotions and intuition. So it could be said that there is contextual support for discussing the potential use of AI, software programs forensic investigations of ESI, for decision-making of corporate directors.


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. The unusual behaviors are identified through such tools as statistical models and mathematical algorithms, so that an entire population of data can be analyzed. There have been several successful prosecutions involving medical fraud as well as the smuggling of goods, both of which involve proving a level of intent to commit the illegal act.

A corporate director could also face allegations of fraud from shareholders or the corporation. The data to be mined may be a smaller pool than millions of electronically billed medical records. Instead, primary sources of ESI may be emails, documents and telephone calls about specific transactions. Breach of fiduciary claims do not involve as rigorous an element of criminal intent, as gross negligence or merely the failure to act in good faith is a basis for plaintiff’s claims. If the more challenging criminal fraud cases in document scope and evidentiary proofs have brought successful prosecutions, then data mined evidence of illegal behavior is quite plausible against corporate directors in a breach of fiduciary duty case.

A corporate director’s breach of fiduciary duties may also stem from illegal acts, such as violations of the Foreign Corrupt Practices Act, backdating options to enhance value and price for the director, or acts that evidence misleading, inaccurate, or fraudulent reporting of financial statements.

Perhaps just as much as omen, albeit outside of existing litigation, is the use predictive behavior analytics to characterize the type of judgment used by corporate directors when voting by proxy. At issue was whether voting data can be used to predict value judgments by the directors, specifically whether they were more favorable to the firm-generated proposals as opposed to minority shareholder proposals.

In the proxy project, a “Voting Analytics” database was compiled that includes voting records for all (3,540) funds across top 104 fund families. The database included a merge of voting

173 MBCA § 8.30(a).
174 See American College of Trial Lawyers, Recommended Practices for Companies and Their Counsel in Conducting Internal Investigations, 46 Am. Crim. Rev. 73 (2009) which discusses when outside counsel should be retained by public companies for internal investigations of suspected wrong-doing by corporate executives.
175 Lilian Ng, Qinghai Wang, and Nataliya Zaiats, Do Mutual Funds Vote Responsibly? Evidence from Proxy Voting.
data for all mutual fund investors with a certain type of information, which was then refined by the software programmers to a dataset sampling of 8,929 proposal-firm observations.\textsuperscript{176}

One finding was that “mutual fund managers tend to vote more in favor of management than shareholder-sponsored proposals”\textsuperscript{177} 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”.\textsuperscript{178} The conclusion from those findings was that “mutual funds do not demonstrate strongly [socially] responsible voting”.\textsuperscript{179}

If it is possible to use predictive behavioral analytics to find corroborative findings about voting judgments by proxy, it may be equally possible to establish findings that show value judgments or predispositions in voting by a director or a board of directors. 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 interests of the shareholders or the corporation, they could bring a fiduciary claim. This type of predictive analytics to show biases by directors 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 request for production of documents by plaintiffs who have alleged a breach of fiduciary duty or fraud by that very Board.

**Securities Claims**

A potential companion of fiduciary duty claims against directors is securities violations claims. As with fiduciary duty claims, shareholders can allege the directors and/or their corporation have acted in a way that violates the statutory duty fully disclosure material information to potential investors so they can make informed decisions.\textsuperscript{180}

Such claims are related to fiduciary claims in that a securities violation (not fully advising potential and existing shareholders about negatives about the company, and therefore its stock) is similar to shareholders asserting that director’s failure to disclose that information misled them or was a fraud perpetrated on shareholders. A securities violation also exists for profiting from the sale of company stock outside of required reporting disclosures.\textsuperscript{181} That same occurrence is grounds for a breach of a duty of loyalty, and usurping a corporate opportunity. Hence, both

\textsuperscript{176} Id., at 12.
\textsuperscript{177} Id., at 13
\textsuperscript{178} Id., at 15.
\textsuperscript{179} Id., at 22.
securities fraud and breach of fiduciary duty claims are but multiple counts in the same complaint from the same overall facts.

In *Pension Committee*, 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 plaintiffs brought suit under the federal securities laws and under New York law against former directors, administrators, the auditor, and the prime broker and custodian of the Funds. The litigation focused on e-discovery issues, with the court holding that plaintiff failed to meet its discovery obligations to timely impose a litigation hold and preserve relevant documents. The plaintiffs formed an ad hoc committee to investigate the issues prior to filing suit. Presumably plaintiffs were well aware of cases like *Gutman, U.S. Dist. LEXIS 97707, 2008 WL 5084182*, where a default judgment was entered 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. Similar motivations, tactics and claims are easily envisioned by shareholders against corporate directors for fiduciary breaches, which can include the same factual basis for securities fraud.

Fraud claims have also been alleged where electronic documents of plaintiff’s key executive were also required to be produced in a case, despite his claims that the defendant committed fraud in violation of Rule 10-b-5 of the Securities Exchange Act of 1934. There is no reason provided in the case to prevent the parties to be reversed, requiring the defendant from producing electronic documents if the facts were ripe for that issue to be decided.

The Danger of Adverse Inferences

The possibility exists that recovered emails give rise to inferences adverse to a director. Though the inference is not predictive of future behavior it may be even more damaging. If a fact finder is allowed to conclude that the failure of a director to produce emails regarding his correspondence with a competing company, that inference may go to the heart of plaintiffs’ claim that the director had conflicts of interest or secretly profited from this relationship with that competing company. The case below illustrates the possibilities.

A director’s sale of stock may also give rise to adverse inferences based on ESI that is problematic to a director. As noted in the above chart, the corporate sale of stock is clearly within the realm of fiduciary duty claims where shareholders allege impropriety in the purpose or methods by a key executive in the transaction. In *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co, Inc.*, an e-discovery dispute arose when a parent company with stock in its subsidiary sued Morgan Stanley for fraud in connection with the parent’s sale of stock in the

---

182 *Pension Committee*, at 462.
183 Id.
184 Id.
185 Id.
subsidiary. The parent company was to receive in return stock of an unrelated third company (Sunbeam). The parent alleged that Morgan Stanley had knowledge of a fraudulent scheme by Sunbeam.

The relevance of forensic analytics is that central to plaintiff’s case was the need to show Morgan Stanley’s knowledge of the illicit scheme. Plaintiff therefore aggressively sought discovery of defendant’s ESI. Morgan Stanley produced approximately 1,300 pages of emails. Thousands of backup tapes were analyzed by an outside vendor. But after repeated failures of defendant to fully produce emails and backup tapes, noncompliance with the court’s discovery orders, and apparent destruction of ESI, the court granted plaintiff’s request for an adverse inference against Morgan Stanley, the non-producing defendant.

The adverse inference is just another of the potential pitfalls awaiting a director facing claims of fiduciary error. In Coleman, the Order carefully stated the scope of the inference. Specifically, the Order stated that the Court shall provide the jury “conclusive” findings of fact. No inferences were to be drawn from those facts, but “counsel may make such argument to the jury in favor of whatever inferences the evidence may support.” The evidence would likely include the results from plaintiff’s forensic expert. As noted above, deliberate attempts at destruction of documents can be detected or recovered. If the documentary evidence (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 Sunbeam 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 he breached his fiduciary duty by using that information to secretly profit at the expense of the corporation.

The Coleman Order further allowed the plaintiff to argue that any concealment by Morgan Stanley of the Sunbeam transactions “is 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 ESI that contained damaging information is not produced to the plaintiffs.

Another adverse inference case is J.P. Morgan Chase Bank v Liberty Mutual Ins., where the insurance company was sued for allegedly guaranteeing payments in case of Enron’s bankruptcy. The Court admitted emails from certain senior bank officials, but additionally determined that jurors could use those emails as probative of defendant’s claim that the transactions in question

---

187 2005 WL 679071 (Fla. Cir. Ct), Case No. 502003CA005045XXOCAI, p. 1.
188 2005 WL 679071 (Fla. Cir. Ct), Case No. 502003CA005045XXOCAI, p. 7.
189 2005 WL 679071 (Fla. Cir. Ct), Case No. 502003CA005045XXOCAI, p. 7. Emphasis supplied by author.
190 2005 WL 679071 (Fla. Cir. Ct), Case No. 502003CA005045XXOCAI, p. 7.
were not insurable.\textsuperscript{191} While this is a use of recovered emails that brings favorable inferences to the defendant company, it is just as possible that recovered emails may bring damaging information to light. A court may have jury instructions that allow an adverse inference against a defendant. In essence then emails were used to suggest behavior- guarantees made - not directly shown from evidence. The defendant could be a corporate director and plaintiffs may likewise use recovered emails to establish that the director made guarantees of corporate actions, and that it would be breach of contract and fiduciary duty to renege on that promise.

**Even with Maximum Director Protections**

To present the most challenging aspect of this issue, assume that a hypothetical company will choose to incorporate in a state that maximizes the liability shield affordable to its board of directors and key executives. The state of choice is Delaware which nearly extinguishes all fiduciary duties by the directors if the organization’s governing documents so state. 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.\textsuperscript{192} There are a few notable exceptions. Section 102(b)(7) further states the liability shield does not exist:

“...(i) For any breach of the director’s duty...(ii) for acts or omissions not in good faith or which involve intentional misconduct or a knowing violation of law...(iv) for any transaction from which the director derived an improper personal benefit.”

These requirements of good faith and avoidance of adverse improper personal benefit are still within the various hypothetical presented in this article. Corporate directors should be just as wary of the potential use of forensic evidence under the Delaware statutes as the MBCA-based scenarios presented above.

To this foundation of director restrictions, we add a likely interpretation that the fiduciary duty must expand if necessary so that the director has awareness of modern theories of overseeing assets. In *Brane v Roth*, the court held that directors of a grain cooperative breached their fiduciary duties by retaining a manger inexperienced in “hedging” – the cutting edge practice of hedging or reducing the risk to company assets through the use of derivative securities.\textsuperscript{193} 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…”\textsuperscript{194}

\textsuperscript{191} 2002 WL 31867731 (S.D.N.Y. Dec 23, 2002) The lack of insurability was because the transactions were classified “off-the-books”.


The corporation gained ninety percent of its income from long grain transactions, and the failure of the directors to employ accepted hedging techniques caused damage to the company. Most relevant to this article is the court’s decision that the practice of hedging was a legitimate business expectation.\(^{195}\)

The reasonable business expectation of shareholders of a corporation should, in this author’s view, increase as the state of 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 email-sifting algo’s 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 bring a breach to those 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 ESI. Arguably, directors that do not know the basics or know enough to supervise those with the forensic responsibility have breached their duty. 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.\(^{196}\) While the trustees’ fiduciary standard is termed 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.\(^{197}\) The prudent investor standard, as with corporate fiduciary duty rules, includes a requirement of reasonable knowledge by the trustee.\(^{198}\) But academic literature also suggests the need for a trustee to have a “working” knowledge of modern theories on how to manage a beneficiary’s portfolio is required.\(^{199}\)

So the directive that a director view his duty based on a prudent person “in similar circumstances” should include those attuned to the technological advances of forensic tools that discover financial reporting errors within a CRM system, or other tools of investigation of email irregularities as found with DEDICOM.


\(^{197}\) The prudent investor rule requires a trustee to be reasonable knowledgeable or have professional advice on behalf of a beneficiary. See Borkus, note 53, p. 138.


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 what they say they are.200 One corrective technology in response to the corporate scandals of the 2000s (Enron, WorldCom, Tyco, Qwest, and HealthSouth) is the increased identification of a practice termed CEM – cosmetic earnings management. One example is when unmanipulated income below a certain key user reference is artificially placed just above the threshold.201 For example, $499 million in earnings is changed to reflect $501 million in earnings. While the actual amount of earnings difference could be viewed as relativity minor, the sole purpose of the technique is “deception with the intent of swaying user judgment.”202 Even minor increases in income can bring significant increases in company value based on market perceptions.203

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 the wheelhouse of a director’s constructive knowledge or oversight.204 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 is therefore also on the immediate responsibility of those directors. The impact of such technology is actually two-fold: The 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.

The Impact of Social Media

A director, bluntly stated, could 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

---

200 The director’s oversight functions are repeatedly and broadly stated in Section 8.30. See MBCA § 8.30(b) and MBCA § 8.30(c). 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. MBCA § 8.30(e). Subsection (e) of that section clarifies that reliance is not allowed if the director knows that reliance is unwarranted. MBCA § 8.30(e). By necessary implication therefore, the judgment required to determine whether reliance is warranted is part of the oversight function of a director.


202 Charles E. Jordan and Stanley J. Clark, Detecting Cosmetic Earnings management Using Benford’s Law, The CPA Journal, p 32,37 (February 1, 2011). Another example is where a depreciable asset’s useful life is extended thus increasing the income that can be reported. See Charles E. Jordan and Stanley J. Clark, Detecting Cosmetic Earnings management Using Benford’s Law, The CPA Journal, p 32,33 (February 1, 2011) for several other examples of cosmetic earnings manipulation.


204 See Charles E. Jordan and Stanley J. Clark, Detecting Cosmetic Earnings management Using Benford’s Law, The CPA Journal, p 32,33 (February 1, 2011) for several other examples of cosmetic earnings manipulation.
significant bits of information can be learned from his use of that App unbeknownst to him. That 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. And perhaps a director’s excesses or judgmental improprieties that were latent, 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.

Media analysts have already concluded that the internet changes the way people think and communicate. 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.” 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 – reappeared even though he deleted the search from his computer, or used a wiping utility in efforts to eliminate it from the deleted files of his hard drive.

CONCLUSION

This article concerns the risks of shareholder lawsuits for a director breach of fiduciary duties. This article outlines various emerging challenges heretofore not generally contemplated or litigated concerning that issue. As a species, humans may well be creatures of habit. If so, then in this age of artificial intelligence and forensic analytics, the deviation from the habit can be more readily flagged than ever before with digital anomalies and a host of software programs that create algorithms. The consequences are likely to be more adverse for the deviant corporate director attempting to avoid breach of fiduciary duty claims than before this digital age.

For the scrupulous corporate director, there may also be an increased responsibility to be knowledgeable of modern technology to remain reasonable in judgment and oversight. This could especially be exposed if the director’s own company retains forensic experts.

---

205 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 data mine information about their users and provide the information to third parties without disclosure to the phone user. See AMIR EFRATI, SCOTT THURM and DIONNE SEARCEY, Mobile-App Makers Face U.S. Privacy Investigation, Wall Street Journal, April 5, 2011, http://online.wsj.com/article/SB10001424052748703806304576242923804770968.html (last visited July 13, 2011).


208 The more expansive impact of social networks on corporate directors and executives is subject of a future article by this author, “Corporate Directors Caught in the Web of the Internet and Social Media”.

43
A greater concern for directors involving forensic experts is whether they are prepared for the arms race to convince the court of its own forensic protocol. The studies to date evidence a general unpreparedness for e-discovery in over half of the corporations reviewed. This article presents numerous scenarios illustrating the potentially devastating consequences in personal liability to a director if the forensic arms war is lost.