Minnesota Journal of Law, Science & Technology

Volume 11 | Issue 2 Article 6

2010

Corporate Cyborgs and Technology Risks

Andrea M. Matwyshyn

Follow this and additional works at: https://scholarship.law.umn.edu/mjlst

Recommended Citation
Andrea M. Matwyshyn, *Corporate Cyborgs and Technology Risks*, 11 MINN. J.L. SCI. & TECH. 573 (2010).
Available at: https://scholarship.law.umn.edu/mjlst/vol11/iss2/6

The Minnesota Journal of Law, Science & Technology is published by the University of Minnesota Libraries Publishing.

Matwyshyn AM. Corporate Cyborgs and Technology Risks. *Minnesota Journal of Law, Science & Technology*. 2010;11(2):573-98.

Corporate Cyborgs and Technology Risks

Andrea M. Matwyshyn*

I. INTRODUCTION

The law has long treated corporations as persons with rights, and it continues to expand this treatment.[1] In a similar vein, in technology contexts, the practical differentiation between human persons and corporate persons grows tenuous in many respects. Today's corporations seem more enmeshed in our daily reality, more anthropomorphic and "friendly." The local radio station wants to be your Facebook friend. The Twitter feed of your favorite coffee chain intermingles with feeds authored by your human friends. Internally, however, corporations are becoming progressively less "human"; they are relying less upon the particular human employees that fill the physical space of the corporate headquarters and relying more upon their information systems. This seeming contradiction of internal mechanization with external humanization calls to mind the metaphor of a "cyborg"—a hybrid creature that is part machine and part human.

This shift in corporate identity toward a cyborg identity warrants new legal consideration: the shift has carried with it technology driven risks to both individual entities and the economy as a whole. This article argues that, as companies progressively shift to a blended human-machine identity, dangers lurk from overzealous technology adoption without strong audit mechanisms and oversight. Historical examples warn us that organizations sometimes adopt technology overzealously, prior to the consideration of the full implications of this adoption. Using the securities industry as a case study

---

© 2010 Andrea M. Matwyshyn.

* Andrea M. Matwyshyn is an Assistant Professor of Legal Studies & Business Ethics at The Wharton School at University of Pennsylvania. She can be reached at amatwysh@wharton.upenn.edu.

1. *See, e.g.*, Citizens United v. Fed. Election Comm'n, 130 S. Ct. 876, 913 (2010).

of cyborg transformation, this article points to the historical example of the Books and Records Crisis that plagued the securities markets in the 1960s and 1970s and required SEC intervention. Drawing lessons about technology mismanagement from this crisis, it raises questions regarding today's technology reliant corporations. In particular, this article raises questions with regard to information management and information security. The piece concludes by calling for an information accountability regime with more meaningful internal and external corporate oversight that more effectively blends regimes of corporate, securities, contract, intellectual property, tort and criminal law.

II. THE RISE OF THE CORPORATE CYBORG: MECHANICAL INTERIOR WITH A HUMAN FACE

Cyborgs have been a fixture in science fiction literature,[2] movies,[3] and technology theory for decades.[4] Part machine and part human, they embody two types of creatures. On the one hand, cyborgs can be humans who have extended their capabilities through technology enhancement to their bodies, such as two professors who have surgically attached various gadgetry to their bodies.[5] On the other hand, cyborgs can be machines that have a decidedly human appearance and are capable of generating human emotional connections to them, such as the fictional Terminator from the movie series of the same name.[6] Corporations today appear to be evolving into this second type of cyborg—a machine with a human appearance capable of generating emotional connections.

---

2. *See, e.g.*, MARTIN CAIDIN, CYBORG (1972).

3. Perhaps the most widely recognizable cyborg character from popular culture is that of Arnold Schwarzenegger's Terminator character from the movie series of the same name. The Terminator appeared as a human to the outside world in a conventionally attractive physical form and functioned relatively effectively in a world of humans in pursuing its goals. It was also capable of winning humans' trust. However, upon closer examination, his behaviors gave away the truth of his interior: he was, first and foremost, a machine programmed with certain preferences and directions. THE TERMINATOR (Orion Pictures 1984).

4. For a discussion of cyborg theory, see generally CHRIS GRAY, THE CYBORG HANDBOOK (1995).

5. *See, e.g.*, Lisa Guernsey, *At Airport Gate, A Cyborg Unplugged*, N.Y. TIMES, Mar. 14, 2002, at G4; Kevin Warwick, The University of Reading, http://www.kevinwarwick.com/ (last visited March 10, 2010).

6. THE TERMINATOR, *supra* note 3.

As the types of assets that dominate many companies have moved away from tangibles toward intangibles,[7] corporate structure has also evolved. Internally, a corporation conceptualizes itself as a type of machine—a series of overlapping information networks, both human and technological. Externally, a corporation seeks to be viewed as a trusted (human) friend to maximize its goodwill. Internal corporate information flows are increasingly mechanized through computerization; externally, however, corporations work to maintain a human face to build brand and customer loyalty. On one hand, companies are struggling with growing into heavily technology-driven structures of information management,[8] but on the other, they still view the external projection of human characteristics as being of foremost business importance.

A. INTERNAL MECHANIZATION

Companies are increasingly internally mechanized; information management and computer systems are driving dramatic change inside companies. Businesses have become progressively more technology-centric and, consequently, organized in large part around their unifying computer systems. Since Time Magazine named "The Computer" as its person of the year in 1983,[9] corporations' reliance on information systems has increased significantly, as have the capabilities of those systems. This integration of information technology into corporate operations during the last two decades has changed the ways that companies handle information—both sensitive internal information and personally identifiable consumer information.[10]

---

7. For example, goodwill alone frequently makes up over 15 percent of corporate assets in large companies. *Get Out the Red Pen*, BARRON'S, Feb. 16, 2009, http://online.barrons.com/article/SB123457702581886857.html?mod=wsjcrmain.

8. *See* Jim Carr, *From RSA: Financial Services Companies Struggling with Multichannel Authentication,* SC MAGAZINE, Apr. 10, 2008, http://www.scmagazineus.com/From-RSA-Financial-services-companies-struggling-with-multichannel-authentication/article/108906/.

9. *Cover*, TIME, Jan. 3, 1983, *available at* http://www.time.com/time/covers/0,16641,19830103,00.html.

10. Further, as internet purchases became a regular part of consumer economic behaviors in the late 1990s, a new economic environment emerged.

Companies have increasingly centralized sensitive corporate information:[11] trade secret information,[12] financial information,[13] business partner and customer information is centralized in companies' internal computer systems. This centralization arose because businesses sought to solve communication problems among various parts of the company, and overcoming these communication obstacles across machines became a corporate priority for many organizations.[14] The goal was, therefore, to allow all parts of the organization to effectively interact with each other and communicate internal data.[15] Business communications progressively shifted from

---

The defining characteristic of this new commercial environment has been widespread corporate collection, aggregation, and leveraging of personally identifiable consumer data with the assistance of information systems. Consumers increasingly venture online to engage in information-sensitive activities, such as checking bank balances or transmitting credit card information in connection with purchases. *See* SUSANNAH FOX ET AL., TRUST AND PRIVACY ONLINE: WHY AMERICANS WANT TO REWRITE THE RULES 13, 15 (2000), http://www.pewinternet.org/~/media//Files/Reports/2000/PIP_Trust_Privacy_Report.pdf. Many companies today hoard data for marketing and other purposes. They collect as much information as possible about their customers in the name of targeting products more effectively and generating secondary streams of revenue through licensing their databases of consumer information. H.R. Rep. No. 106-74, pt. 3, at 106–07 (1999).

11. For example, most law firms use document management systems to centralize work product. For a discussion of document management software, see Dennis Kennedy & John Gelagin, *Want to Save 16 Minutes Every Day?,* FINDLAW, Feb. 1, 2003, http://technology.findlaw.com/resources/scripts/printer_friendly.pl?page=//articles/00006/009973.html. This use of information technology serves to facilitate knowledge management, the sharing of institutional intellectual resources such as form contracts, and control over access to certain information. *Id.*

12. For a discussion of the risks that trade secret information faces from technology, see, for example, Elizabeth A. Rowe, *Saving Trade Secret Disclosures on the Internet Through Sequential Preservation*, 2007 B.C. INTELL. PROP. & TECH. F. 091101, at 4 (2007), http://bciptf.org/index.php?option=com_content&task=view&id=31&Itemid=30.

13. The Gramm-Leach-Bliley Act specifically considers the implications of corporate uses of financial information. *See* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in scattered sections of 12 and 15 U.S.C.).

14. These attempts to centralize built in high dependencies between systems. *See, e.g.*, Wayne Labs, *Machine Control: Still Islands of Automation?*, FOOD ENGINEERING, Jan. 2006, at 97, 97–99.

15. In the context of manufacturing, this meant connecting up "islands of automation" into a single communication network. *See id.*

real space to virtual space,[16] and entirely new technology-contingent information businesses have arisen, such as eBay and Google.[17] Even the most traditional of companies began to experiment with internet sales through company websites. Increasing computerization and automation of businesses generated enterprise-wide computing.

B. EXTERNAL HUMANIZATION

Corporations have gone to great lengths to anthropomorphize their images in order to generate consumer trust and brand loyalty. They engage in philanthropy[18] and advertise in ways that are intended to create interpersonal connection between the brand and the customer. Recently, these advertising outreach efforts have extended to social networking websites such as Facebook. In 2008, approximately $1.6 billion was spent on U.S. online social network advertisements.[19] Business enterprises have pages,[20] friends,[21] fans,[22] and send and receive messages through social networks; they participate as any human would. If content creation can be used to judge impact, these personification efforts appear to

16. *See, e.g.*, Ed Frauenheim, *Report: E-mail Volume Grows Rapidly*, CNET NEWS, Oct. 2, 2003, http://news.com.com/2110-1032-5085956.html?tag=3Dnefd_hed (last visited May 7, 2010) (noting an 80% growth in volume of corporate email between 2002 and 2003).

17. Sharon K. Sandeen, *The Sense and Nonsense of Website Terms of Use Agreements,* 26 HAMLINE L. REV. 499, 508 (2003). As a consequence of this transformation, numerous state corporate statutes have been amended to allow for email notice, virtual shareholder meetings, and internet proxy voting. Gary W. Derrick & Irving L. Faught, *New Developments in Oklahoma Business Entity Law*, 56 OKLA. L. REV. 259, 263 (2003); Robert C. Pozen, *Institutional Perspectives on Shareholder Nominations of Corporation Directors*, 59 BUS. LAW. 95, 102–03 (2003).

18. *See, e.g.*, Terry Timm Moos, Cisco Systems Honored with 2005 Excellence in Corporate Philanthropy Award, (Feb. 27, 2006), http://newsroom.cisco.com/dlls/2006/hd_022706b.html.

19. Rachael King, *Building a Brand with Widgets*, BUSINESSWEEK, Mar. 3, 2008, http://www.businessweek.com/technology/content/feb2008/tc20080303_000743_page_2.htm.

20. *See, e.g.*, Facebook: Starbucks, http://www.facebook.com/Starbucks (last visited Mar. 9, 2010).

21. *See, e.g.*, Boystown Live, http://www.boystownlive.com (last visited Mar. 9, 2010).

22. Ben and Jerry's has over one million fans on Facebook. *See* Facebook: Ben & Jerry's Homemade, Inc., http://www.facebook.com/benjerry (last visited Mar. 9, 2010).

be working—hundreds of user generated pages about companies,[23] products,[24] corporate officers[25] and corporate characters have been created.[26] Corporate "characters" or branded mascots, in particular, have engendered numerous hate groups[27] and fan groups[28] where people discuss their emotional reactions to these characters, just as they do with regard to human celebrities.[29] For example, the change of the eTrade spokesbaby during the 2010 Superbowl resulted in an almost instantaneous internet outcry.[30] These technology-based extensions of the corporate person are becoming increasingly important in marketing efforts and goodwill generation. The last fifteen years have brought a dramatic transformation to the structure, outreach and internal dynamics of companies. In 1995, internet browsers were a novelty. In 2010, almost every company feels compelled to maintain an internet presence and offer multiple technology-aided forms of communication. No

23. *See, e.g.*, Facebook: Microsoft, http://www.facebook.com/Microsoft?ref=search&sid=100000695049406.1033447816..1 (last visited Mar. 10, 2010).

24. *See, e.g.*, Facebook: i am a pc and ……SHUT UP!!, http://en-gb.facebook.com/pages/i-am-a-pc-and-SHUT-UP/321665282894 (last visited Mar. 10, 2010).

25. *See, e.g.*, Facebook: I HATE BILL GATES, http://www.facebook.com/group.php?gid=4836749570&ref=search&sid=100000695049406.3743157703..1 (last visited Mar. 10, 2010).

26. *See, e.g.*, Facebook: E*TRADE Baby, http://www.facebook.com/search/?q=etrade+baby&init=quick#!/etradebaby?ref=search&sid=1247199379.932930107..1 (last visited Mar. 15, 2010).

27. *See, e.g.*, Facebook: I hate Clippy, http://www.facebook.com/search/?flt=1&q=clippy&o=65&sid=605538877.2002331308..1&s=0#!/group.php?gid=303574911105&ref=search&sid=605538877.1987303274..1 (last visited Mar. 10, 2010).

28. *See, e.g.*, Facebook: R.I.P. Clippy 1997-2007, http://www.facebook.com/pages/RIP-Clippy-The-Microsoft-Paper-Clip/103394899696284 (last visited Mar. 10, 2010).

29. *See, e.g.*, Facebook: Lady Gaga, http://www.facebook.com/ladygaga (last visited Mar. 15, 2010).

30. *See, e.g.*, Tanya Irwin, *New Etrade 'Baby' Arrives During Super Bowl*, MEDIADAILYNEWS, Jan. 15, 2010, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=120739; James Poniewozik, *James Brown Takes One for the Team*, TUNED IN (Jan. 25, 2010, 10:05 AM), http://tunedin.blogs.time.com/2010/01/25/james-brown-takes-one-for-the-team/; digitalLouisville.com, What Louisville Is Saying About… E-trade, http://www.digitalouisville.com/keyword/e-trade (last visited Mar. 9, 2010); Love the E Trade Baby, http://www.experienceproject.com/groups/Love-The-E-Trade-Baby/193839 (last visited Mar. 9, 2010).

longer are consumers simply reading advertisements; they are interacting with companies in many of the same ways they interact with humans online. Real time chat agents are available for immediate questions.[31] Call centers frequently staffed by agents, even if located in another country, are a Skype call away. Consumers increasingly feel that even feel that companies are "following" them too closely using technological means online—much like a nosy neighbor or a paparazzo might in real life.[32]

As one might assume, a fundamental tension exists between these two trends of progressive mechanization and simultaneous humanization. This tension, consequently, is leading to management failures. However, unlike most other types of management failures, information management failures frequently negatively impact not only the entity itself, but also negatively impact other technologically-connected entities.[33] Thus this tension in corporate cyborg identity has given rise to new information privacy, security and legal concerns.

III. TECHNOLOGY RISKS, FAILS, AND CORPORATE CYBORGS

Although companies are aggressively marching forward in their technology adoption and reliance, they sometimes neglect to build the internal management infrastructure necessary to use new technologies responsibly. These management failures result in ignoring or unwittingly assuming significant technology risks that can meaningfully damage corporate assets and goodwill. In other words, technology mismanagement can undercut companies' own efforts as anthropomorphized identities. One industry that provides an example of this corporate struggle between mechanization and

---

31. *See, e.g.*, Dell – Hardware Chat, http://support.dell.com/support/topics/global.aspx/support/chat/hardware_chat?c=us&cs=19&l=en&s=dhs (last visited Apr. 25, 2010).

32. Douglas MacMillan, Facebook Privacy Policies Draw Criticism by 15 Consumer Groups, May 6, 2010, BUSINESSWEEK, http://www.businessweek.com/news/2010-05-06/facebook-privacy-policies-draw-criticism-by-15-consumer-groups.html (last visited May 7, 2010).

33. For a discussion of the "shared secret" nature of information and the transitive effects of data breaches, see, e.g., Cem Paya, Quasi-secrets, Chapter 9 in ANDREA MATWYSHYN (ED.), HARBORING DATA (2009).

humanization is the securities industry.

A. THE SECURITIES INDUSTRY BOOKS AND RECORDS CRISIS: A CASE STUDY OF "FAILS"

In technology slang, the term FAIL refers to an impressive failure—meaning a failure that is impressive for all the wrong reasons. Frequently preceded by the word "epic,"[34] a FAIL is used to describe events evidencing an extraordinary level of incompetence, stupidity or bad luck.[35] However, the original use of the word "fail" actually referred to a failed securities transaction during a notorious and embarrassing period in securities history known as the Books and Records Crisis. The Crisis was marked by extreme levels of technology mismanagement and deficient risk assessment: as new technology was introduced on exchanges and within brokerages, a clash between new computerized elements and the preexisting human elements resulted. The Books and Records Crisis served as a harbinger of the struggles of today's corporate cyborgs.

1. The History of the Crisis

The Books and Record Crisis refers to the 1967–1971 period where over five billion dollars worth of "fails"—trades that were not properly settled[36]—threatened to destabilize the securities industry and exchanges.[37] Described by industry insiders as a "terrifying and unending nightmare,"[38] the crisis arose in part because the securities industry failed to successfully evolve in response to the introduction of the critical pieces of technology by the New York Stock Exchange (NYSE), which resulted in greatly increased trading volume.[39] While

34. For examples of epic FAILS, see FAIL Blog, http://failblog.org/ (last visited March 9, 2010).

35. *See id.*

36. Brokers were required to deliver physical certificates that were signed and notarized within five days of executing a trade to "settle" the trade. Because of the complexity of the bureaucratic process required post-trade, certificates frequently failed to materialize by the deadline. Wyatt Wells, *Certificates and Computers: The Remaking of Wall Street, 1967 to 1971*, 74 BUS. HIST. REV. 193, 203 (2000).

37. *Id.* at 203–07.

38. These were the words of a partner in a Chicago brokerage. *Id.* at 207.

39. These technologies included the 900 Ticker, the radio paging system, and the full automation of floor data in 1964–1966. *See* NYSE Euronext,

brokerages struggled to maintain trusted relationships with clients, their internal technology mismanagement undercut these efforts. This crisis resulted in significant part from the overzealous implementation and use of new technology on exchanges and in brokerages without considering the risks and outcomes. In the words of one author, the brokerage houses reflected "scarcity of individuals of managerial ability and talent" and many of the largest brokerages lacked any system of internal audits.[40] Thus, when new trading technologies started to be introduced on exchanges, firms could not successfully adapt to handle record trading volume post-trade, and, in 1968, record trading volume on exchanges and in over-the-counter markets began to outstrip brokerage houses' ability to keep up in their records. Brokerage houses began trading at rates faster than their own employees could settle the transactions post-trade.[41] Instead of investing in expansion or cutting down trading rates to a level the firms could settle, many brokerages simply chose to ignore the problem and continue trading. Aggressive trading was perceived to be the best strategy for securing large returns;[42] the rest of operations were deemed a lower priority.

Records of brokerages became plagued with the notation "DK" which stood for "Don't Know about the transaction," indicating that errors existed somewhere in the trading process. Even brokerages that worked to keep their records in order were negatively affected by the inadequacies of other firms. Because firms traded with each other regularly on an exchange floor and over the counter, if one broker's failed recordkeeping resulted in the inability to settle a trade, both brokers suffered a "fail."[43] In the words of one study, "[t]he operations sins of one company were visited upon others."[44]

Timeline, http://www.nyse.com/about/history/timeline_1960_1979_index.html (last visited Mar. 15, 2010).

40. Wells, *supra* note 36, at 198.

41. An antiquated system of transferring ownership existed: stock certificates needed to be signed, notarized and physically transferred. Brokers needed to process this paperwork and keep accurate records on transfers. The purchase or sale of a single security might require as many as sixty-eight separate tasks and an error anywhere in the process would result in a failed transaction. *Id.* at 201.

42. *Id.* at 200–01.

43. *Id.* at 206.

44. *Id.* at 207.

Although NYSE began to urge members to correct their internal problems, by the spring of 1968, the SEC reached the conclusion that inadequate pressure existed to motivate firms to rectify backlogs of failed trades.[45] In July 1968, the SEC asserted that "[i]t is a violation of the anti-fraud provisions of the federal securities laws . . . for a broker to buy a security . . . for a customer if the broker-dealer has reason to believe that he will not be able to deliver the security."[46] Despite the threats of regulatory action, firms continued to insist that they could meet their obligations and adapt their operations to new technologies. It became apparent, however, that these assertions were, at best, irrationally optimistic when NYSE sent its own staff to audit some of the delinquent firms. NYSE later used its own funds to shut down some of these brokerages when these audits demonstrated large scale improprieties and deficits in management.[47]

The firms that were not shut down by the exchange and SEC regulators turned to computerization of records to solve the recordkeeping debacles.[48] These firms viewed computers as a panacea—the "magic solution"[49] to solve their prior failures in management. However, few insiders actually knew how to use the new machines effectively, and they failed to understand their limitations.[50] Computers were not capable of restoring order to years of recordkeeping chaos; they were limited in their organizational ability by the humans who used them. In the words of technologists, "Garbage in, garbage out."[51] Further, serious software malfunctions exacerbated the difficulty of the automation process,[52] and firms sometimes began relying on computer systems before these systems had been properly vetted for malfunctions.[53] In line with this overly exuberant reliance on the new machines, firms dismissed some of their senior clerks, causing glitches to result in even more serious problems in the books. In the words of the SEC, "[w]hen

45. *Id.* at 208.
46. *Id.* at 209.
47. *Id.*
48. *Id.* at 210.
49. *Id.*
50. *Id.*
51. *Id.*
52. *Id.*
53. *Id.*

firms . . . began to automate, they experienced substantial problems."[54] In the case of one brokerage, it was a computer error concealing approximately $7.5 million in liabilities that caused the SEC to demand immediate corrective action[55] and ultimately led to the firm's demise.[56] In summary, only computers could process the new volumes of transactions, but they were costly and only as good as their operators and programmers. Further, small firms could not afford to automate with computers.[57] This group of factors led to a period of consolidation among firms[58] and to billions of dollars of mishandled trades that were never entirely straightened out. As a result of the Crisis, the Securities Investor Protection Corporation, a government-owned corporation, was created. [59]

2. Lessons from the Crisis

The Books and Records Crisis can be analyzed as a harbinger of the types of severe systemic consequences technology mismanagement can cause in data intensive industries; these risks are amplified for today's cyborg corporations. Specifically, analysis of the Books and Records Crisis offers six lessons. First, technology adoption choices and management by an interconnected business partner impacts every member of the web of interconnection. When NYSE adopted new technologies that dramatically expanded trading volume capability, it resulted in a technology-driven ripple effect in the brokerages that were interconnected with the exchange. Mismanaged brokerages' internal technology failures destabilized the recordkeeping of other brokerages, including the records of brokerages that were well-managed.

Second, when financial incentives to hide technology inadequacy are significant, firms will sometimes lie about the

---

54. *Id.* at 211 (quoting *Securities Market Agencies: Hearing Before the Subcomm. On Commerce and Finance of the H. Comm. on Interstate and Foreign Commerce,* 91st Cong. 143 (1969)).

55. *Id.* at 228.

56. *Id.* at 233.

57. *Id.*

58. *Id.* at 234.

59. SIPC is governed by a seven-member board, with members appointed by the Treasury secretary, the chair of the Federal Reserve Board and the President. It was funded by a levy on securities transactions and was supported by a $1 billion line of credit from the federal treasury. Three members of the board were to come from the securities industry. *Id.* at 226.

extent of their managerial competence. Firms may believe it to be in their self-interest to knowingly or recklessly exacerbate harm to the other members of the interconnected web of companies and to individual consumers. Audit and regulatory oversight is essential to preserving accurate information. In the case of the Crisis, firms asserted their ability to rectify trades in the face of evidence to the contrary until independent NYSE and SEC auditors confirmed otherwise.

Third, automation and technology are never a panacea; they are always limited by the human error and skill of the people who build and maintain systems. As firms turned to technology during the Crisis to solve their inability to settle trades on the back end, they realized that their prior limitations of imperfect recordkeeping could not be rectified by computers. Programming and data entry errors came with financial consequences.

Fourth, companies should always expect new technologies to fail and be prepared to compensate with redundancy measures. Thus, a business strategy predicated on perfect implementation and operation of a computer system will inevitably lead to large scale failure. When computer errors occurred during brokerages' implementation of new systems, because the senior clerks with the requisite knowledge to otherwise compensate for the lost data had been fired, no backup system existed. The results were multi-million dollar computer errors that could have been mitigated with a backup system.

Fifth, dramatic changes in technology always create winners and losers, frequently driven by specialized knowledge and capital resources. The most dangerous failure in technology implementation is a failure to accurately assess knowledge deficits inside an organization. As many brokerages found out when they failed during the Crisis, businesses that incorrectly analyze management deficits and risks may not survive dramatic technological change. Further, technology evolution is capital intensive and leads to elimination of small firms that lack the corporate coffers to automate to the extent of large firms.

Finally, regulatory responses can be successful. As the SEC's response to the Crisis demonstrates, the destabilizing effect of new technologies can be mitigated through thoughtful oversight and audit. The key to regulatory response is

identifying problems early.

B. CORPORATE CYBORGS AND INFORMATION SECURITY

The technology management deficits of today's corporate cyborgs are perhaps most immediately visible in the context of information security and intangible asset management. Companies are processing sensitive information about themselves and their customers, relying on their computer systems to a high degree, but these companies are simultaneously plagued by human errors—errors in programming and errors in technology management. Rather than projecting the "trustworthy" human face they seek to project, companies frequently unintentionally generate an untrustworthy one. Shortfalls in corporate information security and data handling practices illustrate this tension and its unintended negative consequences. Empirical data from surveys of corporate officers[60] and rampant data breaches of millions of records in 2009 speak for themselves—even the most sophisticated companies demonstrate widespread inadequacies in information security management.[61] Meanwhile, as the recent hacking of Google and approximately thirty other technology companies demonstrates,[62] not even the

60. Empirical data demonstrates that companies are not anticipating and managing information risk. For example, in 2008 in an annual information security survey by PriceWaterhouseCoopers of over 7,000 respondents who comprised CEOs, CFOs, CIOs, CSOs, vice presidents and directors of IT and information security from 119 countries, at least three of ten respondents could not answer basic questions about the information security practices of their organizations. PRICEWATERHOUSE COOPERS, SAFEGUARDING THE CURRENCY OF BUSINESS: FINDINGS FROM THE 2008 GLOBAL STATE OF INFORMATION SECURITY STUDY 2 (2008). Thirty-five percent did not know the number of security incidents in the last year; 44% did not know what types of security incidents presented the greatest threats to the company's most sensitive information, assets and operations; 42% could not identify the source of security incidents; 67% said their organization does not audit or monitor compliance with the corporate information security policy—whether the attack was most likely to have originated from employees (either current or former), customers, partners or suppliers, hackers or others. Id. at 15.

61. *See, e.g.*, Privacy Rights Clearinghouse, Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Jan. 30, 2009).

62. *See, e.g.*, Kim Zetter, *Google Hackers Targeted Source Code of More Than 30 Companies*, WIRED, Jan. 13, 2010, http://www.wired.com/threatlevel/2010/01/google-hack-attack/ (last visited May 7, 2010).

most sophisticated of technology companies are immune from penetration by a driven group of attackers. Each breached record is attached to a company or a consumer potentially harmed by the disclosure. As the negative publicity following information security breaches at companies such as the TJX Companies[63] and Heartland[64] demonstrates, mismanagement of information systems can dramatically undercut the efforts of a company to build a trusted human face with the outside world.

Meaningful enterprise-wide oversight is necessary to create a culture of information security. Returning to the case study of the securities industry, although major players in the securities industry have experienced data breaches in the last five years,[65] some of these entities appear to have failed to acknowledge the importance of information security. Of the brokerages that have experienced breaches few, if any, have an officer-level position dedicated to information management. Chief information officers and chief security officers are usually missing from their rosters of officers. Meanwhile, these same entities increasingly rely on technology to replace humans in making trading decisions.

Approximately only three percent of the trading volume on the NYSE is done by means of traditional "open outcry" trading with humans; 97% of NYSE trades are executed using electronic communication networks.[66] Trading floors, in the opinion of some experts, remain in existence only for show, as a relic of prior trading times to pose for news cameras.[67] In the last three or so years, trading reliant on computer algorithms

63. Mark Jewell, *TJX Breach Could Top 94 Million Accounts*, MSNBC, Oct. 24, 2007, http://www.msnbc.msn.com/id/21454847/ (last visited May 7, 2010).

64. Jaikumar Vijayan, *Heartland Data Breach Could Be Bigger Than TJX's*, INFOWORLD, Jan. 21, 2009, http://www.infoworld.com/article/09/01/21/Heartland_data_breach_could_be_bigger_than_TJXs_1.html (last visited May 7, 2010).

65. For example, both Goldman Sachs and UBS have filed charges against former employees stealing code from proprietary trading platforms. Katherine Heires, *UBS Charges 3 Ex-Employees with Code Theft*, SEC. INDUSTRY NEWS, July 14, 2009, http://www.securitiesindustry.com/news/-23668-1.html (last visited May 7, 2010).

66. *See* Jon Stokes, *The Matrix, but with Money: the World of High-Speed Trading*, ARS TECHNICA, July 28, 2009, http://arstechnica.com/tech-policy/news/2009/07/-it-sounds-like-something.ars (last visited May 7, 2010).

67. *Id.*

has dramatically increased:[68] high frequency trading accounts for approximately 60% of trading volume, and this number is expected to rise.[69] Average daily volume has increase by 164% since 2005, according to the NYSE, because of the activities of "a handful" of traders.[70] Some commentators believe serious concerns exist over whether the practice of high frequency trading itself might be a market manipulation,[71] and case studies show that the prices of shares purchased by other "slow" traders are influenced in a detrimental manner to make more profit for the high frequency trader.[72] According to an NYSE Euronext official, over 90% of orders submitted to the New York Stock Exchange by firms using high-frequency trading are canceled.[73] Others insist that high frequency trading is a desirable practice that enhances market exchanges. The SEC has opened an investigation into the practice.[74]

Regardless of which position one accepts, what is indisputable is that the information security of the transactions and the management of the machines performing them create potential for serious market disruption and provide an attractive target for information criminality. In a business environment where even the most sophisticated technology companies fall victim to information criminals compromising their source code,[75] the securities industry is certainly not

---

68. Kristi Oloffson & Stephen Gandel, *High-Frequency Trading Grows, Shrouded in Secrecy*, TIME.COM, Aug. 5, 2009, http://www.time.com/time/business/article/0,8599,1914724,00.html#ixzz0hiZW3PDT (last visited May 7, 2010).

69. *High-Frequency Trading Surges Across the Globe*, SYDNEY MORNING HERALD, Dec. 2, 2009, http://www.smh.com.au/business/highfrequency-trading-surges-across-the-globe-20091202-k5yw.html (last visited May 7, 2010).

70. *See, e.g.*, Charles Duhigg, *Stock Traders Find Speed Pays, in Milliseconds*, N.Y. TIMES, July 23, 2009, at A17.

71. *Id.* (describing how slow trading firms were subject to different prices because of high frequency trading activities by other firms).

72. *See, e.g.*, *id.*

73. Jonathan Spicer & Herbert Lash, *Who's Afraid of High-Frequency Trading?*, REUTERS, Dec. 2, 2009, http://www.reuters.com/article/idUSN173583920091202 (last visited May 7, 2010).

74. David Scheer, *SEC Probes Manipulation by 'Advanced Trading Systems'(Update 1)*, BLOOMBERG, Sept. 10, 2010, http://www.bloomberg.com/apps/news?pid=20601103&sid=aGenyVbVDd2A (last visited May 7, 2010).

75. For example, Google was recently targeted by a highly sophisticated

immune from information security risks. Further, as a whole, because of the current shallowness of the information security talent pool, it is also likely to be less skilled in defending itself than would be a sophisticated technology company.[76]

As the previous discussion of the Books and Record Crisis articulated, the securities industry reflects a history of problematized information handling. However, whereas the previous information problems of the Crisis were driven by internal inadequacies, now the information threats are driven in part by external criminals. Hackers have successfully stolen sensitive information from securities firms, including logins and social security numbers, and have executed unauthorized trades, in at least one case worth over $700,000.[77] In fact, the list of entities that have experienced information security breaches during the last five years includes firms engaged in high frequency trading.[78] Although some firms' business relies in significant part of computerized trading, firms engaged in high frequency trading do not always have a Chief Security

---

group of hackers who sought to gain access to its source code and that of approximately thirty other companies. *See, e.g.*, Zetter, *supra* note 62.

76. When attempting to find qualified candidates to staff information security management positions, the current candidate pool is not large due to the demands of the field. For a discussion of the qualifications of information security management professionals, see, for example, Jessica Twentyman, *How Can IT Experts Make a Successful Move to a Career in Information Security?,* SC MAGAZINE, Feb. 25, 2010, http://www.scmagazineuk.com/how-can-it-experts-make-a-successful-move-to-a-career-in-information-security/article/164504/ (last visited May 7, 2010). There is also a general perception among technology professionals that working in research and development in a technology company is "cooler" than working for a financial services company, where their influence on corporate policy and products may be limited or information security may be a low priority.

77. The SEC recently instituted an enforcement action against LPL Financial after hackers obtained clients' unencrypted names, addresses and social security numbers, compromising the logon passwords of 14 financial advisers and four assistants. The SEC fined LPL $275,000 and required that LPL strengthen its security safeguards with respect to customer information; the hacker(s) placed, or attempted to place, more than $700,000 in trades in securities of nineteen different companies. LPL Financial Corp., Exchange Act Release No. 58515, Investment Advisor Act Release No. 2775, 94 SEC Docket 170 (Sept. 11, 2008), *available at* www.sec.gov/litigation/admin/2008/34-58515.pdf.

78. *See, e.g.*, Kim Zetter, *FBI: Russian Programmer Stole Stock-Trading Secret Code*, WIRED, July 6, 2009, http://www.wired.com/threatlevel/2009/07/aleynikov/ (last visited May 7, 2010).

Officer or Chief Information Officer with technical expertise to meaningfully assess quality of their code and their information risk.[79] Meanwhile, source code for at least three proprietary high frequency trading platforms has already been stolen by rogue insiders,[80] and other points of vulnerability almost certainly exist in these systems. Computer code is never perfect.

All computer systems are vulnerable to security problems and attacks, including trading systems.[81] A skilled attacker on a vulnerable system can sometimes cause the owners of those systems to lose control of their machines.[82] In light of the high volume of trades that rely on the integrity of high frequency trading platforms, an injection of rogue code into a single proprietary high frequency trading platform could have a meaningfully negative impact on the market. Unraveling the millions[83] of trades of a high frequency platform gone haywire across the world's markets[84] could cause disruption to not only the firm using the corrupted platform itself but the markets as

---

79. For example, despite Goldman Sachs's recent information security breach, based on the Goldman Sachs website as of this writing, no executive-officer-level position focused on information security risk appears to exist in their governance structure, and no background information in the current executive officers management team points to computer science expertise sufficient in this author's opinion to generate an impression of adequate skill to meaningfully oversee high frequency trading operations. *See, e.g.*, Goldman Sachs, Our People: Executive Officers, http://www2.goldmansachs.com/our-firm/our-people/leadership/executive-officers.html (last visited Apr. 8, 2010). In a market where 97% of trading is computer mediated, it can be argued that this is a significant management deficit.

80. *See, e.g.*, Katherine Heires, *Code Green: Goldman Sachs & UBS Cases Heighten Need to Keep Valuable Digital Assets from Walking Out the Door. Millions in Trading Profits May Depend on It.*, SEC. INDUSTRY NEWS, July 20, 2009, http://www.securitiesindustry.com/reports/19_75/-23696-1.html?zkPrintable=true (last visited May 7, 2010); David Kravets, *Second Banker Accused of Stealing High-Frequency Trading Code*, WIRED, Apr. 20, 2010, http://www.wired.com/threatlevel/2010/04/bankerarrested/#ixzz0nEvwPB6u (last visited May 7, 2010).

81. *See* Stokes, *supra* note 66.

82. *See, e.g.*, Ryan Naraine, *Patch Tuesday Heads-Up: 8 Bulletins, 5 Critical*, ZDNET (Apr. 9, 2009, 11:06 AM), http://blogs.zdnet.com/security/?p=3116.

83. High frequency traders frequently trade thousands of shares each millisecond. *See, e.g.*, Duhigg, *supra* note 70.

84. High frequency trading is increasingly international. *See, e.g.*, *High-Frequency Trading Surges Across the Globe*, *supra* note 69.

a whole. Share price changes do not happen in a vacuum; other firms will have traded on the market information that resulted from the tainted high frequency trades.

Particularly if we consider these information security failures in historical context—in the context of an industry known to have a history of deficient recordkeeping and management practices that have already once caused the multi-billion dollar Books and Records Crisis in our markets[85]—market integrity concerns arise. There is reason to question whether stringent information security practices are in place with respect to these companies' proprietary trading platforms. Additionally, some of the companies engaging in high frequency trading and making markets are private companies not subject to extensive SEC oversight.[86] High frequency trading with inadequate information security presents a meaningful risk of market instability, potentially with FAILS surpassing even the billions of dollars of "fails" of the Books and Records Crisis period.[87]

Thus, the securities industry demonstrates the unsustainable tension of many corporate cyborgs: while seeking to generate feelings of trust in consumers and striving to put forth a human face on their enterprises through spokespeople such as the popular character of the eTrade baby,[88] the last five years demonstrate a dramatic shift in the industry toward eliminating humans from the equation in favor of reliance on autonomous and automated computer systems. The rise of high frequency trading as a dominant trading strategy is the product of the cyborg transformation in the industry, and its dangers loom large beneath the technologies' surfaces and the companies' anthropomorphic exteriors.

---

85. *See* Wells, *supra* note 36, at 203.

86. Just as the Crisis caused a recalibrating of power in the securities industry in favor of a technocracy where only the strong survived, another such wave of technocratic purging may be in its nascence. *See, e.g.*, Liz Moyer & Emily Lambert, *The New Masters of Wall Street*, FORBES, Sept. 21, 2009, at 40, 41 http://www.forbes.com/forbes/2009/0921/revolutionaries-stocks-getco-new-masters-of-wall-street.html (last visited May 7, 2010).

87. Wells, *supra* note 36, at 203.

88. The eTrade baby's advertising confederates are the subject of a recent commercial misappropriation lawsuit by actress Lindsay Lohan. *See, e.g.*, Kieran Crowley, *Lindsay Lohan Wants $100M over E-Trade Ad*, N.Y. POST, Mar. 9, 2010, at 5.

IV. INFORMATION ACCOUNTABILITY

In the previous sections, this article has introduced a fundamental tension between the human face and the computerized innards of today's corporation. It has argued that both historical examples and current practices evidence significant potential for harms to arise from mismanagement of this tension. In other words, a deficit in information accountability exists.

The law has been slow to drive meaningful improvements to this information accountability deficit. Although the data breach notification regime which currently exists in over forty-five states significantly raised awareness of the risks of information vulnerability, the level of information care inside enterprises has not necessarily dramatically improved. In fact, as the capabilities of the systems they use increase, the information risks that pertain to them become more substantive. As such, the tension between external and internal corporate identity will continue to escalate.

A larger reconsideration of the bodies of law governing the intersection of companies and information technology is warranted. Such a reconsideration includes updating multiple traditional bodies of law to reflect the changed technology reality of today's companies—corporate law, securities law, contract law, intellectual property law, tort law, and criminal law.

A. CORPORATE LAW

Two important shifts are needed in corporate law to address the regulatory challenges presented by today's cyborg corporations. First, the law needs to acknowledge that the value of corporate information assets is generated at least in part through their economic and social embeddedness. Thus, corporate law needs to acknowledge the interweaving of information privacy from the consumer side and information security from the corporate side. Data collection is a choice that brings with it technology risks; it is not a necessity. Because consumers cannot foresee future corporate uses of their information or accurately assess the skill of companies' information management, they rely on the expertise of the data holders to protect them from harm. For example, databases of information about consumers and their preferences are corporate assets but, by definition, remain connected to the

human subjects of that data. If mishandled, these databases can harm the consumers whose data resides in them. Those companies that choose to aggregate and share this information should be deemed to owe a legal duty of stewardship to the subjects of the data collection.[89] It is common that in situations where consumers place their trust in a specialized service provider that the law creates a type of regulated industry or registration regime. For example, in Delaware, over forty various professions are regulated under Title 24 of the Delaware Code because each presents unique risks to consumers.[90] So too the law should approach companies that engage in information processing.

Second, as I have argued elsewhere,[91] the rise of internal corporate mechanization and the corresponding heavy reliance on intangible assets requires the law to rethink fiduciary duties. Fiduciary duties need to shift toward a paradigm of ongoing management rather than their current focus on limited oversight of extraordinary transactions.[92]

B. SECURITIES LAW

Although the Sarbanes-Oxley Act took steps to recognize the importance of information integrity in an organization with respect to financial statements, its more aggressive posture

89. A parallel might be drawn to a researcher being obligated to protect the identities and data of human subjects in her research.

90. The Division of Professional Regulation in Delaware regulates the following professions: accountancy, realtors, landscape architects, architects, real estate appraisers, podiatrists, mental health counselors, chemical dependency professionals, chiropractors, funeral service providers, pilots, veterinarians, dentists, psychologists, electricians, geologists, adult entertainment, speech/language pathologists, audiologists, hearing aid dispensers, doctors, dieticians, nutritionists, respiratory care professionals, social workers, acupuncturists, manufactured home installers, plumbing/heating/ventilation/air conditioning/refrigeration professionals, cosmetologists, barbers, nursing home providers, occupational therapists, massage and bodywork professionals, optometrists, boxers and sparring exhibition providers, pharmacists, possessors of controlled substances, physical therapists, land surveyors, private investigators, private security agencies, bail enforcement agents, pawnbrokers, secondhand dealers and scrap metal processors. *See* DEL. CODE ANN. tit 24, §§ 101–5505 (2005 & Supp. 2008).

91. *See* Andrea M. Matwyshyn, *Imagining the Intangible*, 34 DEL. J. CORP. L. 965, 967 (2009).

92. *Id.* Specifically, the duty of good faith and the duty of care should be modified to include concerns over ongoing management of intangible assets.

towards audit of information assets has not, in practice, gone far enough with respect to information care. As the discussion of the securities industry in earlier sections highlights, information handling practices leave room for improvement even at the most sophisticated companies. Specifically, securities law can be strengthened in at least two ways: first, mandating CIOs or CISOs for all public companies and financial services providers within the SEC's regulatory reach, and second, clarifying materiality standards for disclosure of information security breaches and risks.

First, the SEC should mandate that every public company and financial services provider within its regulatory reach must designate a chief information officer or chief information security officer, granting such position meaningful decision-making authority to oversee information handling inside the company as a whole. Just as the Health Insurance Portability and Accountability Act required that all covered entities create an officer-level position to consider the privacy implications of the health data that the entity controls,[93] so too securities law should approach concerns over information handling among all public companies and financial services providers. In a world where 97% of trading on leading exchanges is done computer to computer,[94] and particularly in circumstances where an organization is experimenting with technology-driven practices such as high frequency trading, an officer level pool of experts with adequate technological training to meaningfully oversee and internally audit (and attest to the quality of) these practices should be mandatory. Further, the SEC should devote serious study to the systemic information inequalities[95] and new risks that technology mediated practices such as high frequency trading introduce into the system. The potential for malicious actors to partially destabilize our markets through compromised computer code in trading platforms is a real threat and such a large scale attack is, perhaps, merely a matter of time.

Second, the SEC should clarify requirements with respect to the materiality of disclosing information security breaches

93. Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. § 1320d et seq.,

94. Stokes, *supra* note 66.

95. Granting rights to some but not other players to co-locate servers may present technology equity concerns.

inside public companies. As I have argued elsewhere,[96] disclosure practices of companies with respect to information security breaches and risks vary even within the same industry. Further, the diminished value of their assets following a data breach may not always be reflected in lowered share price in the market. The SEC must take a more aggressive lead in creating a culture of information accountability in our markets.

C. THE RELATIONSHIP AMONG INTELLECTUAL PROPERTY LAW, CONTRACT LAW, TORT LAW AND CRIMINAL LAW

The internal mechanization of companies increases their reliance on technology and intangible assets. This reliance also means that companies' interest in aggressively protecting their intellectual property increases in tandem. As a consequence, they now sometimes rely on more proactive contract, tort and criminal law postures when they perceive their intellectual property to be at stake, emboldened by the uncertainties of the Digital Millennium Copyright Act[97] and the Computer Fraud and Abuse Act,[98] in particular. This strategic shift requires clarifying the balance among intellectual property, contract, tort and criminal law.

While working to maintain a trusted human face, companies progressively shift new risk onto their customers and employees through contract and related legal approaches. Contracting practices demonstrate new knowledge imbalances between drafters and consumers and have become progressively more imbalanced in favor of the drafter over time.[99] Rights of recourse upon breach are being interpreted in different manners by different courts. In practice, consumers lack any meaningful ability to negotiate contracts for most digital products and services; the law should rebalance the

---

96. *See* Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation,*. 3 BERKELEY BUS. L.J. 129, 173–83 (2005).

97. Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 5, 17, 28 and 35 U.S.C.).

98. 18 U.S.C. § 1030 (2006).

99. *See, eg.*, Andrea M. Matwyshyn, *Chapter 4: Mutually Assured Protection: Development of Relational Internet Data Security and Privacy Norms*, *in* ANUPAM CHANDER ET. AL., SECURING PRIVACY IN THE INTERNET AGE (2008).

power balance in the relationship away from the corporate drafter.

Although the companies employing or providing various technologies should know about any risks associated with their use, they sometimes fail to adequately test these products[100] or perceive themselves to lack a duty to disclose risks of use in detail meaningful to users.[101] For example, since the adoption of the Digital Millennium Copyright Act, companies frequently rely on digital rights management (DRM) technologies to protect their intellectual property. These DRM technologies sometimes make alterations to users' systems in ways that aren't apparent to users; these changes are sometimes neither technologically transparent nor clear from the way the contracts governing use of the product describe the DRM. As I have argued elsewhere,[102] this shift toward greater information parity can occur in part through creation of a more robust construction of consent, one predicated on a reasonable digital consumer standard. Similarly, though not all courts currently enforce privacy policies as contracts, privacy policies should indeed be enforced as contracts, and their breach should provide basis for a breach of contract action and damages. This approach, when coupled with data breach notices, would offer one method for recourse in instances of information mismanagement. Blanket protection from contract damages and tort liability for digital products and services creates incentives for lack of care on the part of companies.

Further, many companies do not consider themselves obligated to address or mitigate the digital harms that arise

---

100. Recently, Google's Buzz product caused uproar among consumers and privacy groups when, after only internal testing, the product was launched. In its initial incarnation, Google Buzz incorporated users' Gmail contacts by default in an opt-out model. An FTC complaint and at least one civil suit have been filed in the United States, and Canada's privacy commissioner has asked for an explanation of the company's conduct. *See, e.g.*, Thomas Claburn, *Google Buzz Stung by Lawsuit*, INFORMATIONWEEK, Mar. 8, 2010, http://www.informationweek.com/news/security/privacy/showArticle.jhtml?articleID=223200135 (last visited May 7, 2010).

101. One such incident involved digital rights management code used by Sony in connection with music discs. See, e.g., J. Alex Halderman & Edward W. Felten, *Lessons from the Sony CD DRM Episode*, 15 PROC. USENIX SECURITY SYMP. 1, 1 (2006), available at http://cse.umich.edu/~jhalderm/pub/papers/rootkit-sec06.pdf.

102. *See* Andrea M. Matwyshyn, *Technoconsen(t)sus*, 85 WASH. U. L. REV. 529, 566 (2007).

from use of their products or services. As I have also argued elsewhere,[103] a reasonable expectation of code safety should be created with respect to licensors of digital products, as should a duty to protect, correct and update problematic or vulnerable code. The "harm" that arises in such a situation is in part the failure to warn.

However, when considering the digital harm itself rather than a failure to warn, complicating questions can arise when considering a civil remedy for information mismanagement, particularly with respect to quantifying damages and the relationship with criminal law. In some cases, plaintiffs allege that a breach of contract can lead to both a tort based remedy and, potentially, a criminal prosecution. A circuit split currently exists on questions regarding the intersection of employment contacts, information breaches and civil and criminal computer intrusion.[104] Just as in tort and criminal law generally, what constitutes an intrusion or an unwanted technological "touching" of a user's machine is contingent entirely on user consent. The language used by computer intrusion statutes revolves around "interception," i.e. monitoring without consent, and "exceeding authorized access," meaning surpassing the extent of consent.[105] Two federal statutes, as well as a patchwork of state statutes, use this framework of consent in the context of criminal and civil computer intrusion – the Electronic Communications Privacy Act[106] (ECPA) and the Computer Fraud and Abuse Act.[107] The

103. *See* Andrea M. Matwyshyn, *Hidden Engines of Destruction: The Reasonable Expectation of Code Safety and the Duty to Warn in Digital Products*, 62 FLA L. REV. 109, 136–45 (2010).

104. *See* LVRC Holdings LLC. v. Brekka, 581 F.3d 1127, 1137 (9th Cir. 2009) (holding employee use of employer information does not constitute violation of Computer Fraud and Abuse Act). *But see* Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 421 (7th Cir. 2006) (holding employee use of employer information constitutes violation of Computer Fraud and Abuse Act).

105. *See infra* notes 106 & 107.

106. Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

ECPA is composed of Title I, amendments to the Wiretap Act, 18 U.S.C. A. §§ 2510–2522 (West 2000 & Supp. 2009), and Title II, the Stored Communications Act, 18 U.S.C.A. §§ 2701-2711 (West 2000 & Supp. 2009). Generally, the Wiretap Act prohibits interception of communications, including those in transient storage. "Except as otherwise specifically provided in" the Act, "electronic communication[s]," which are defined expansively, may not be "intercepted." § 2511(1)(a). An exception is provided for electronic

balance among these four legal regimes – intellectual property, contract, tort and criminal law – and the meaning of "consent" must be crafted carefully to avoid turning mere breaches of contract into a basis for criminal prosecutions.

V. CONCLUSION

This article has argued that a progressive transformation has occurred in companies: today's companies reflect a hybrid machine and human existence – a type of corporate cyborg identity. Anthropomorphized entities reliant on their computer

---

communication service providers, but it only applies to "activity which is a necessary incident to the rendition of [the] service or to the protection of the rights or property of the provider of that service." § 2511(2)(a)(i). The Stored Communications Act restricts accessing communications that reside in a particular system. The U.S. Patriot Act clarified at least one existing possible ambiguity in the language of the Stored Communications Act, explicitly including voicemail messages under its coverage. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, 283 (codified as amended at 18 U.S.C. § 2703 (2006)). The Stored Communications Act's main criminal provision reads as follows: "(a) Offense. -- Except as provided in subsection (c) of this section whoever-- (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished. . . ." 18 U.S.C.A. § 2701(a) (West 2000 & Supp. 2009). The Stored Communications Act contains an explicit "provider" exception: "Subsection (a) of this section does not apply with respect to conduct authorized -- (1) by the person or entity providing a wire or electronic communications service." § 2701(c). It has been argued that this § 2701(c)(1) establishes almost complete immunity for a service provider that "obtains, alters, or prevents authorized access to" e-mail that is "in electronic storage" in its system. *See* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114-15 (3d Cir. 2003) ("[W]e read § 2701(c) literally to except from Title II's protection all searches by communications service providers."). A second provision of the Stored Communications Act prohibits "a person or entity providing an electronic communication service to the public [from] knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service." § 2702(a)(1). This provision also has service provider exceptions, permitting a provider to give access to an electronic communication "to a person employed or authorized or whose facilities are used to forward such communication to its destination," § 2702(b)(4), or "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service," § 2702(b)(5). Some confusion exists regarding the interaction of the two statutes and certain potential definitional ambiguities. Most recently the interaction of the two parts of the ECPA was discussed in United States v. Councilman, 418 F.3d 67 (1st Cir. 2005).

107. 18 U.S.C. § 1030 (2006).

systems, today's companies rely heavily on intangible assets. Because of this reliance, they use and experiment with technological advancement. Sometimes this experimentation is done imprudently. Thus, today's cyborg companies introduce new types of technology risks and exacerbate pre-existing tensions in law. Using historical and modern examples from the securities industry, this piece has argued in favor of crafting a regime of information accountability: changes to corporate, securities, intellectual property, contract, tort and criminal law are needed to address these new risks that accompany today's corporate cyborgs.